

## **Beschlussempfehlung und Bericht**

### **des Ständigen Ausschusses**

#### **Zu**

- a) der Mitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg vom 18. Januar 2018**
  - Drucksache 16/3290
  - **33. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg für die Jahre 2016/2017**
  
- b) der Mitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg vom 21. Februar 2018**
  - Drucksache 16/3600
  - **1. Informationsfreiheits-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg für die Jahre 2016/2017**

#### **Beschlussempfehlung**

Der Landtag wolle beschließen,

- a) der Mitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg vom 18. Januar 2018 – Drucksache 16/3290 – und der vom Innenministerium hierzu mit Schreiben vom 26. April 2018 vorgelegten Stellungnahme der Landesregierung (siehe Anlage 1 zum Ausschussbericht) – Kenntnis zu nehmen;
  
- b) von der Mitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg vom 21. Februar 2018 – Drucksache 16/3600 – Kenntnis zu nehmen.

07. 06. 2018

Der Berichterstatter:

Reinhold Gall

Der Vorsitzende:

Dr. Stefan Scheffold

Ausgegeben: 13.06.2018

*Drucksachen und Plenarprotokolle sind im Internet  
abrufbar unter: [www.landtag-bw.de/Dokumente](http://www.landtag-bw.de/Dokumente)*

*Der Landtag druckt auf Recyclingpapier, ausgezeichnet mit dem Umweltzeichen „Der Blaue Engel“.*

## Bericht

Der Ständige Ausschuss beriet die Mitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg vom 18. Januar 2018, Drucksache 16/3290, in Verbindung mit dem Schreiben des Innenministeriums vom 26. April 2018 (*Anlage 1*) sowie die Mitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg vom 21. Februar 2018, Drucksache 16/3600, in seiner 33. Sitzung am 7. Juni 2018. Gleichzeitig nahm der Ausschuss den Mündlichen Bericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg gemäß § 31 Absatz 3 Satz 4 des Landesdatenschutzgesetzes sowie den Mündlichen Bericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg gemäß § 12 Absatz 3 des Landesinformationsfreiheitsgesetzes in Verbindung mit § 31 Absatz 3 Satz 4 des Landesdatenschutzgesetzes entgegen.

Der Ausschussvorsitzende erklärte, zunächst gehe es um den Bereich Datenschutz.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit legte dar, er freue sich, den ersten Tätigkeitsbericht aus dem Datenschutzbereich vorstellen zu können, den er selbst verantworte. Hinsichtlich Aufbau und Art der Darstellung habe er sich im Wesentlichen an dem von seinem Amtsvorgänger verantworteten letzten Bericht orientiert, den er im vergangenen Jahr vorgestellt habe; denn nach seiner Wahrnehmung seien die bisherigen Berichte auf positive Resonanz gestoßen. Neu sei, dass es direkt hinter dem Vorwort nunmehr eine Rubrik „Schwerpunkte“ gebe, um die Lesbarkeit des Berichts noch etwas zu steigern und um klarzumachen, wo aus Sicht seiner Dienststelle die besonderen Herausforderungen im Bereich des Datenschutzes in den Jahren 2016 und 2017 gelegen hätten.

Im Folgenden gehe er vertiefend auf die Bereiche Datenschutz-Grundverordnung, die seine Dienststelle bereits in den vergangenen Jahren intensiv beschäftigt habe, Beschäftigtendatenschutz und Veränderungen in seiner Dienststelle im Berichtszeitraum ein.

Zum Bereich Datenschutz-Grundverordnung führte er aus, am 25. Mai sei diese in Wirksamkeit getreten und habe gerade für die Aufsichtsbehörde zu einer Aufgabenhäufung geführt. Der Aufsichtsbehörde würden zukünftig weite Aufgaben im Bereich der Aufklärung von Betroffenen, aber auch von Unternehmen zugeordnet. Zusätzlich zu der Beratungstätigkeit, die einen großen Schwerpunkt ausmache, komme die Sanktionierung hinzu. Diese Aufgabenausweitung habe den Landtag im Berichtszeitraum dazu veranlasst, auch die personelle Ausstattung seiner Dienststelle deutlich anzuheben. Für diesen sehr begrüßenswerten Schritt bedanke er sich. Zwischenzeitlich hätten fast alle der neuen Stellen besetzt werden können. Schwierigkeiten habe es lediglich im technischen Bereich gegeben. Denn im Raum Stuttgart sei es sehr schwer, Techniker zu finden, die bereit seien, für die aus deren Sicht „schmale Kost“ einer A-15-Stelle tätig zu werden. Er sei jedoch guten Mutes, dass es gelinge, auch die derzeit noch offene Stelle in diesem Bereich rasch zu besetzen.

Die Rolle seiner Dienststelle ändere sich derzeit grundlegend. Im europäischen Konzert werde seine Dienststelle zukünftig als Aufsichtsbehörde eines Landes eine deutlich andere Rolle wahrnehmen müssen als bislang. Sie sei Teil eines Konzerts der europäischen Aufsichtsbehörden, die sich intensiv miteinander abstimmen. Damit sei die Rolle, die einem Landesbeauftragten zukommen könne, im Wesentlichen dadurch gekennzeichnet, Dolmetscher hinsichtlich der Ansichten, Einsichten oder Problemstellungen zu sein, die sich aus seinem Aufgabengebiet ergäben, und in diesem Zusammenhang insbesondere auch Anregungen für Änderungen oder Ergänzungen der Datenschutz-Grundverordnung zu geben und an den Europäischen Datenschutzausschuss heranzutragen. Damit könne dafür gesorgt werden, dass sich die Datenschutz-Grundverordnung, mit der derzeit die ersten praktischen Erfahrungen gesammelt würden, in eine gute Richtung weiterentwickle. Der baden-württembergische Landesdatenschutzbeauftragte werde die deutschen Datenschutzbeauftragten in einer neuen Arbeitsgruppe auf europäischer Ebene vertreten, die sich ausschließlich mit Social Media befasse. Dabei handle es sich um eine interessante, aber auch sehr anspruchsvolle Aufgabe; denn im Bereich Social Media und Marketing in diesem Zusammenhang seien derzeit wesentliche Umwälzungen im Gange. Auch Tracking sei ein großes Thema. In diesem Bereich

werde seine Dienststelle künftig die deutschen Interessen auf europäischer Ebene vertreten können.

Aus der Beratungstätigkeit seiner Dienststelle vor dem 25. Mai könne er berichten, dass es nicht nur bei Unternehmen eine sehr große Nachfrage gebe, sondern insbesondere auch bei denjenigen, für die die Datenschutz-Grundverordnung zwar Anwendung finde, für die diese jedoch wirklich „schwere Kost“ sei, nämlich die kleinen Unternehmen sowie die Vereine und Verbände, die nahezu unterschiedslos durch die Datenschutz-Grundverordnung in eine neue Pflichtenstellung gebracht worden seien. Dort gebe es intensive Pflichten im Bereich der Information und im Bereich der Bedienung von Betroffenenrechten, die zwar für ein Großunternehmen ganz gut zu bewältigen seien, jedoch für kleinere und mittlere Unternehmen und insbesondere für nicht gewerbliche Vereine eine wirklich große Herausforderung darstellten.

Dort sehe seine Dienststelle eine der Verbesserungsmöglichkeiten mit Blick auf den „One-size-fits-all“-Ansatz der DS-GVO, der auf der einen Seite brillant sei, weil der Vollzug relativ leicht sei, der jedoch bereits zu der Erkenntnis geführt habe, dass es durchaus angemessen sein könnte, stärker zu differenzieren. Es werde auch seine Aufgabe sein, in der Umsetzung und Anwendung der Datenschutz-Grundverordnung zu versuchen, wo immer möglich so zu differenzieren.

Beim Umsetzungsprozess habe sich ein zweiter interessanter Aspekt ergeben. Bekanntermaßen habe der Bundesgesetzgeber relativ rasch mit einem neuen Bundesdatenschutzgesetz reagiert. Nunmehr habe auch der Landesgesetzgeber zeitnah zum 25. Mai entsprechende Änderungen im Landesdatenschutzgesetz vorgenommen. Für den nicht öffentlichen Bereich zeige sich jedoch bereits, dass die getroffenen bundesgesetzlichen Regelungen zu Schwierigkeiten führten. Dort seien zum Teil Verschärfungen vorgenommen worden; es sei also sozusagen auf die Vorgaben der Datenschutz-Grundverordnung draufgesattelt worden, und zwar in einem Bereich, in dem mit zusätzlichen Anstrengungen zum Datenschutz gute Erfahrungen gemacht worden seien, nämlich im Bereich des betrieblichen Datenschutzbeauftragten.

Im Unterschied zur Situation in anderen europäischen Staaten müssten deutsche Unternehmen bereits ab einer niedrigen Schwelle einen betrieblichen Datenschutzbeauftragten bestellen, was sich aus Sicht seiner Dienststelle bewährt habe. Dies habe sich auf der europäischen Ebene in der Diskussion um die Datenschutz-Grundverordnung jedoch leider nicht durchsetzen lassen. Die anderen europäischen Staaten glaubten nicht an das Modell des betrieblichen Datenschutzbeauftragten und hätten deswegen nur eine Optionsmöglichkeit für die Mitgliedsstaaten offengelassen, die, wenn er es richtig sehe, bisher kein anderer Staat außer Deutschland und Österreich genutzt habe. Dies habe zu einer Erschwerung geführt, die aus seiner Sicht jedoch tragbar sei, weil sie erst bei Unternehmen einsetze, in denen sich mehr als neun Personen ständig und regelmäßig mit Datenverarbeitung befassen.

Wenn Unternehmen miteinander konkurrierten, spielten die zusätzlichen Anwendungen für einen betrieblichen Datenschutzbeauftragten zwar eine Rolle, doch rechtfertigten sich diese aus Sicht seiner Dienststelle deshalb, weil sich die Umsetzung der Datenschutz-Grundverordnung ohne interne Hilfe und Unterstützung kaum bewältigen lasse. Er erinnere in diesem Zusammenhang an die Sanktionierungsmöglichkeiten nach der Datenschutz-Grundverordnung, die durchaus als krass zu bezeichnen seien. Denn es könnten Bußgelder in Höhe von bis zu 20 000 000 € bzw. 4 % des weltweiten Jahresumsatzes verhängt werden; derart hohe Bußgelder könne sich kein Unternehmen leisten.

Die Drohung mit Bußgeldern habe bereits Wirkung gezeigt. Sehr viele Unternehmen, die sich dem Datenschutz gegenüber bisher eher reserviert gezeigt hätten, seien nunmehr in die Erfüllung der Datenschutzvorgaben eingestiegen. Ein zusammenfassendes Bild in Bezug darauf, wie die Datenschutz-Grundverordnung umgesetzt worden sei, könne zum gegenwärtigen Zeitpunkt jedoch noch nicht vermittelt werden.

Auch andere Regelungen, die der Bundesgesetzgeber getroffen habe, bereiteten Schwierigkeiten. Beispielsweise sei punktuell versucht worden, die Last der Da-

tenschutz-Grundverordnung zu reduzieren, und zwar in Punkten, die das europäische Recht nicht vorsehe. Beispielsweise dürften die Datenschutzaufsichtsbehörden Ärzte, Anwälte und Steuerberater, also alle Berufsheimnisträger, nicht mehr kontrollieren. Dies sei insbesondere deshalb problematisch, weil die Datenschutzaufsichtsbehörden keine Betretungsrechte mehr hätten und deshalb auch keine Möglichkeit mehr hätten, sich vor Ort Datenflüsse anzuschauen. Auf die Frage an den Bundesgesetzgeber, wer die Berufsheimnisträger kontrolliere, habe es dann geheißen: „Niemand.“ Denn auch die Kammern würden diese Aufgabe nicht übernehmen.

Dies sei offensichtlich eine Lücke, die sich ergebe, mit der sich mit sehr hoher Wahrscheinlichkeit auch der Europäische Gerichtshof beschäftigen werde. Er habe seine Zweifel, dass das Herausnehmen der Berufsheimnisträger aus der Kontrolle Bestand haben werde.

Das Schwierigste an den gesetzgeberischen nationalen Umsetzungsakten zur Datenschutz-Grundverordnung sei aus seiner Sicht, die aus Unternehmenssicht auch bestätigt werde, der Umstand, dass eine erhebliche Rechtsunsicherheit bestehe. Es komme zu einer Situation, in der sich Unternehmen nicht mehr ohne Weiteres darauf verlassen könnten, dass bestimmte Regelungen, die im Bundesgesetzblatt stünden, auch anwendbar seien. Denn es bestehe die Gefahr, dass sich bei genauem Hinschauen ergebe, dass sie mit dem europäischen Recht in Konflikt gerieten. Dieser Konflikt sei rechtlich gesehen relativ einfach aufzulösen. Denn wenn es einen solchen Konflikt gebe, genieße das europäische Recht Anwendungsvorrang, die Datenschutz-Grundverordnung setze sich also durch. Doch in einem solchen Fall setze sie sich in einem Bereich durch, in welchem der rechtsunterworfenen Bürger oder Unternehmer auf das Bundesgesetzblatt vertraut habe und gedacht habe, bestimmte Sachen machen zu dürfen, weil sie dort stünden. Ein Beispiel sei die offenkundig europarechtswidrige Regelung zum Scoring im Bundesdatenschutzgesetz. Die Unternehmen verließen sich darauf und würden in zwei, drei oder vielleicht erst in fünf Jahren vom Europäischen Gerichtshof darüber unterrichtet, dass diese nationale Vorschrift nicht anwendbar sei, weil sie Europarecht widerspreche.

Dies sei eine sehr missliche Situation, und das sei genau das, womit Unternehmen, die durchaus bereit seien, einiges an gesetzlichen Vorgaben hinzunehmen, am schlechtesten umgehen könnten. Denn sie wollten Rechtssicherheit haben und sicher sein, dass das, was es an Normen gebe, klar und verständlich sei und auch in drei oder fünf Jahren noch gelte. Die schwierigen Umsetzungsakte auf Bundesebene hätten jedoch dazu geführt, dass diese Sicherheit verloren gegangen sei, und das sei schlecht.

Zum Bereich Arbeitnehmerdatenschutz führte er aus, in diesem Bereich sei die Zahl der Beschwerden am stärksten gewachsen. Inzwischen bezögen sich die meisten Eingaben auf den Bereich Arbeitnehmerdatenschutz. Dies zeichne nach, dass die moderne Arbeitswelt mit Digitalisierungsfortschritten verbunden sei und die Beschäftigten in vielen Bereichen dem Arbeitgeber gegenüber gläsern würden. Beispiele seien ein PC-Arbeitsplatz, bei dem im Prinzip jeder Tastenanschlag protokolliert werde, oder der Logistikbereich, in welchem selbstverständlich die LKWs getrackt würden, sodass der Arbeitgeber minutengenau und metergenau wisse, wo sich sein Fahrer gerade befinde, ob er vielleicht eine Abkürzung genommen oder eine Rast eingelegt habe. Auch dann, wenn Beschäftigte mit Dienst-Pkw unterwegs seien, die über das Navigationssystem getrackt würden, erhalte der Arbeitgeber Standortdaten, und das führe zu einer ganz anderen Überwachungsqualität, als es sie bisher gegeben habe.

Auch die Videoüberwachung am Arbeitsplatz nehme stark zu; interessant sei, dass beispielsweise im Bereich der Systemgastronomie die Mehrzahl der zahlreichen Kameras nicht auf die Kunden gerichtet seien, sondern auf die Beschäftigten. Auch dies sei eine nicht gute Situation, die für den starken Anstieg der Zahl der Eingaben mitverantwortlich sei.

Seine Dienststelle reagiere auf die gestiegene Zahl der Eingaben im Bereich des Arbeitnehmerdatenschutzes mit einer steigenden Zahl von Fortbildungsangeboten und Einzelveranstaltungen, um dieses Interesse sowohl von Arbeitgeberseite als auch von Arbeitnehmerseite aufzufangen.

Zum Bereich der Arbeit seiner Dienststelle legte er dar, die Zahl der Eingaben an seine Dienststelle habe sich erfreulich entwickelt. Seit 2017 habe sich die Zahl der Eingaben, also der Bitten und Beschwerden von Bürgerinnen und Bürgern beispielsweise über die Meldebehörde, den Arbeitgeber, die Videoüberwachung auf dem Marktplatz oder über das Tracking im Internet, deutlich erhöht. Die Zahl der Eingaben liege inzwischen bei deutlich mehr als 3 000 pro Jahr. Die Entwicklung im laufenden Jahr lasse eine weitere Steigerung erwarten, was sicher auch mit der öffentlichen Diskussion über die Datenschutz-Grundverordnung zusammenhänge.

Einen Anstieg gebe es auch bei der Kontrolltätigkeit seiner Dienststelle, die sich in absoluten Zahlen jedoch in einem sehr überschaubaren Rahmen halte. Während es im Jahr 2016 nur in 16 Fällen möglich gewesen sei, sich die Datenverarbeitung in einem Unternehmen vor Ort anzuschauen, sei im Jahr 2017 versucht worden, diese Zahl zu steigern. Im Ergebnis seien es fast 60 Kontrollen gewesen. Die Zahl werde jedoch dauerhaft niedrig bleiben, weil sich seine Dienststelle schwerpunktmäßig auf die Beratung konzentriere. Sie berate nicht nur die Landesregierung sowie die Behörden im kommunalen Bereich, sondern auch die Unternehmen. Seine Dienststelle berate in letzter Zeit schwerpunktmäßig kleine und mittlere Unternehmen, im Übrigen auch in sehr guter Zusammenarbeit mit den IHKs.

Die wesentlichen Themen der Vorträge oder Schulungen, die seine Dienststelle anbiete, seien die Datenschutz-Grundverordnung, der Arbeitnehmerdatenschutz und das Thema Datenpannen. Letzteres spiele ebenfalls eine große Rolle. Datenpannen müssten der Aufsichtsbehörde seit dem 25. Mai in einem weitaus größeren Umfang gemeldet werden als bisher. Seine Dienststelle habe mit zwischen 30 und 40 Anzeigen pro Jahr gerechnet. Doch in den ersten zwei Wochen nach dem 25. Mai seien bereits über 30 Datenpannen angezeigt worden.

Zur Anzeige von Datenpannen habe seine Dienststelle auf ihrer Homepage ein Tool bereitgestellt, mit dem Pannen unmittelbar eingemeldet werden könnten, und davon werde in viel größerem Umfang Gebrauch gemacht als gedacht. Dabei gehe es nicht nur darum, dass Unternehmen Opfer von Hackerangriffen geworden seien. Vielmehr liege auch dann eine Datenpanne vor, wenn ein Beschäftigter einen Laptop, der leider unverschlüsselt gewesen sei, in der Bahn habe liegenlassen. Auch ein Datenverlust sei in vielen Fällen als Datenpanne meldepflichtig, wenn beispielsweise ein Arzt Teile seiner Dokumentation gelöscht habe und er dem Patienten in der Folge keine vollständige Behandlungshistorie mehr zeigen könne.

Wie dem schriftlichen Tätigkeitsbericht entnommen werden könne, habe seine Dienststelle die Zahl der Schulungen verfünffacht und die Zahl der Vorträge verdreifacht. Seine Dienststelle arbeite also intensiv daran, das Thema Datenschutz nach vorn zu bringen und möglichst laut und intensiv sowie fachkundig darüber zu berichten.

Der Ausschussvorsitzende bedankte sich namens des Ausschusses für diesen mündlichen Bericht und erkundigte sich in seiner Eigenschaft als Abgeordneter danach, was die in Unternehmen erfolgten Kontrollen im Einzelnen erbracht hätten.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit antwortete, im Jahr 2016 habe seine Dienststelle die Chance genutzt, sich schwerpunktmäßig bestimmte Branchen anzuschauen. Auf der Grundlage der Fragestellung, in welchen Bereichen es wohl Probleme bei der Datenverarbeitung geben werde, sei entschieden worden, wo konkret geprüft werde. Einer der Bereiche, der sich angeboten habe, sei der Bereich Callcenter gewesen; denn dort spiele auch der Beschäftigtendatenschutz eine große Rolle. Beispielsweise durch das Mithören von Telefongesprächen durch den Arbeitgeber und seine Mitarbeiter finde dort eine sehr intensive Überwachung statt.

Wenn vor Ort geprüft werde, ergebe sich immer, dass es kein Unternehmen gebe, das, was den Datenschutz angehe, zu 100 % gut aufgestellt sei. Dies wäre im Übrigen auch überraschend; denn dafür seien die Anforderungen inzwischen zu komplex und zu umfangreich geworden. Insbesondere bei der technischen Prüfung, bei der beispielsweise geschaut werde, wie es um die Datensicherheit bestellt sei, wie es mit der Firewall, mit Verfügbarkeitskontrollen oder den technisch-organisatorischen Maßnahmen aussehe, werde seine Dienststelle unabhängig von der Branche und Unternehmensgröße regelmäßig fündig.

Dies hänge u. a. damit zusammen, dass sich auch der Stand der Technik sehr schnell weiterentwickle. In der Datenschutz-Grundverordnung sei die Beachtung des Standes der Technik den Unternehmen jedoch zur Pflicht gemacht worden; das heie, sie mssten in Bezug auf technische Fragestellungen sowie Fragestellungen der Datensicherheit jederzeit à jour sein und immer wieder nachrsten. Wenn dies unterlassen werde, drohten sofort wieder die bereits erwhnten massiven Bugelder. Dies werde auch in den nchsten Jahren ein sehr spannender Bereich werden.

Ein Abgeordneter der Grnen fhrte aus, er bedanke sich beim Landesbeauftragten fr den Datenschutz und die Informationsfreiheit fr den sehr guten Bericht, der deutlich mache, dass es in seiner Dienststelle sehr viel zu tun gebe. Er hoffe, dass der Landtag hinreichend dazu beigetragen habe, die Dienststelle des LfDI fr diese Aufgabe zu rsten. Wenn sich herausstellen sollte, dass die Ressourcen nicht ausreichten, msste er sich melden.

Der Landesbeauftragte fr den Datenschutz und die Informationsfreiheit warf ein, dies wrde er dann gern tun.

Der Abgeordnete der Grnen fuhr fort, der Landtag knne jedoch fr sich in Anspruch nehmen, dass er in den letzten Jahren bereits einiges getan habe, um die Voraussetzungen zu schaffen, dass eine unabhngige oberste Landesbehrde an den Start gehen knne.

In der Folgewoche berichte der Landesbeauftragte fr den Datenschutz und die Informationsfreiheit im Landtag, und daran schliee sich eine Aussprache an. Deswegen knne es in der laufenden Sitzung dabei belassen werden, sich auf Fragen zu beschrnken.

Weiter erklrte er, die Datenschutz-Grundverordnung stehe seit zwei Jahren im Europischen Gesetzblatt, doch alle htten sich irgendwie schlafend gestellt. Er verweise darauf, dass in diesem zwei Jahren von den Nationalstaaten, auch aus der Bundesrepublik Deutschland, in Richtung Brssel relativ wenig passiert sei. Es habe viel Zeit zur Verfgung gestanden, um eine Debatte darber zu fhren, ob die DS-GVO praxistauglich und unternehmensfreundlich oder unternehmensfeindlich sei. Der Zeitpunkt, ab dem die DS-GVO anzuwenden sei und unmittelbar Wirkung in den Mitgliedsstaaten entfalte, habe von Anfang an festgestanden, doch die Debatte ber die DS-GVO habe erst relativ kurz vor dem 25. Mai begonnen.

Er rege an, im Stndigen Ausschuss nach vielleicht einem Dreivierteljahr oder einem Jahr eine sehr kritische Bilanz zu ziehen und in diesem Zusammenhang auch berlegungen darber anzustellen, was getan werden knne, um notwendige Vernderungen vorzunehmen.

Neu sei, dass der LfDI nach dem Marktortprinzip nunmehr zusammen mit anderen Aufsichtsbehrden eine internationale Kontrolle ausbe. Ihn interessiere, ob sich bereits absehen lasse, ob sich diese Aufsicht effektiv wahrnehmen lasse und ob Einfluss beispielsweise auf Unternehmen wie Facebook genommen werden knne.

Der Landesbeauftragte fr den Datenschutz und die Informationsfreiheit uberte, am Anfang sei in der Tat relativ wenig geschehen. Erst als der Termin 25. Mai immer nher gerckt sei, sei die DS-GVO in das allgemeine Bewusstsein gerckt. Es sei normal, dass bestimmte Vernderungen erst in den letzten Wochen oder sogar Tagen vor einem Termin vorgenommen wrden. Fr seine Dienststelle als Aufsichtsbehrde sei es viel wichtiger, zu sehen, dass sich die Unternehmen und Vereine auf den Weg machten, dass sichtbar sei, dass es Bewegung gebe, dass die neuen Rechtsgrundlagen gesehen wrden und dass die Bereitschaft bestehe, sich anzupassen. Es sei zwar rechtlich geboten gewesen, den Stichtag 25. Mai einzuhalten, doch wenn noch ein paar Tage oder Wochen bentigt wrden, sei dies weniger entscheidend als der Umstand, dass sich die Verantwortlichen auf den Weg gemacht htten. Wenn Letzteres dokumentierbar und erkennbar sei, sei das grte Problem behoben.

Seitens Facebook werde wahrgenommen, was auf europischer Ebene beschlossen worden sei und dass in Europa eine Regulierung erfolgt sei, und Herr Zuckerberg stehe auch dem Europischen Parlament Rede und Antwort, was er vor ein paar

Jahren möglicherweise noch nicht getan hätte. Europa sei ein großer und starker Markt und habe mit Millionen von Nutzern ein Potenzial in einer solchen Größe, dass sich auch große Unternehmen durchaus kümmern. Er habe überhaupt keinen Zweifel daran, dass es gelingen werde, für den Fall, dass außereuropäische Anbieter wie Facebook die Datenschutz-Grundverordnung verletzen, wirksame Bußgeldbescheide in die Welt zu setzen; ob es jedoch gelinge, sie letztlich auch zu vollstrecken, sei eine andere Frage. Denn dazu werde die Unterstützung des jeweiligen Sitzlandes benötigt. Er sei sich nicht ganz sicher, wie die USA reagieren würden, wenn beispielsweise gegen Facebook Bußgelder verhängt würden. Bereits in den letzten Jahren habe sich jedoch gezeigt, dass sich auch die großen Unternehmen durchaus an die rechtliche Einschätzung von Aufsichtsbehörden hielten; auch Facebook habe sich bereits zu einem Zeitpunkt an entsprechende Vorgaben gehalten, als es noch nicht möglich gewesen sei, die Umsetzung rechtlich durchzusetzen. Er könne sich nicht vorstellen, warum sich das ändern sollte; die Situation sei durch die Datenschutz-Grundverordnung eher besser geworden.

Er gehe davon aus, dass die meisten Unternehmen und dabei insbesondere die, die aus rechtsstaatlichen System kämen, sich durchaus auch „freiwillig“ an die Anordnungen der Datenschutzaufsichtsbehörden hielten.

Seine Dienststelle sei vom Parlament in die Lage versetzt worden, eine Bußgeldstelle aufzubauen. Dies sei positiv; denn Baden-Württemberg sei das letzte Land in Deutschland, in dem der Landesbeauftragte für den Datenschutz und die Informationsfreiheit selbst keine Bußgelder habe erlassen dürfen. Bußgeldstelle sei das Regierungspräsidium Karlsruhe gewesen. Es habe zwar eine positive Zusammenarbeit zwischen seiner Dienststelle und der Bußgeldstelle gegeben; gleichwohl seien gewisse Reibungsverluste nicht ausgeblieben. Dies sei dadurch, dass seine Dienststelle durch die Datenschutz-Grundverordnung auch zur Ordnungswidrigkeitenbehörde geworden sei, weggefallen.

In seiner Dienststelle gebe es zwei Beschäftigte, die sich auf den Bußgeldbereich konzentrierten. Hierzu sei anzumerken, dass die Beratungstätigkeit von der Bußgeldtätigkeit organisatorisch strikt getrennt sei; denn kein Unternehmen würde Beratungsleistungen in Anspruch nehmen, wenn es befürchten müsste, dass die Beratungsinhalte als Grundlage für Bußgeldverfahren herangezogen würden. Im Bußgeldbereich sei zum einen ein Richter im Wege der Abordnung in seiner Dienststelle tätig, der sich im Rahmen seiner bisherigen richterlichen Tätigkeit speziell mit Ordnungswidrigkeitenverfahren beschäftigt habe. Zum anderen sei ein junger Mitarbeiter eingestellt worden, der bislang anwaltlich tätig gewesen sei. Diese beiden Beschäftigten seien das Team, welches bußgeldwürdige Fälle identifiziere. Dies werde zwar nicht die Schwerpunkttätigkeit des Landesbeauftragten für den Datenschutz und die Informationsfreiheit werden, doch es werde auch zur Tätigkeit dazugehören. Die Aufgabe seiner Dienststelle werde es sein, die richtigen Fälle zu finden, also die Fälle, bei denen bei objektiver Betrachtung Verständnis dafür gewonnen werden könne, dass die Aufsichtsbehörde nicht mehr anders habe reagieren können, als ein Bußgeld zu verhängen. Dies werde eine spannende und anspruchsvolle Aufgabe sein.

Ein Abgeordneter der SPD führte aus, nach seiner Wahrnehmung sei der vorliegende Datenschutzbericht nicht umfangreicher als die vorherigen, obwohl die Arbeit zugenommen habe. Ferner seien ihm bei der Lektüre bisher keine systematischen Verstöße gegen den Datenschutz aufgefallen. Er wolle die Datenschutzprobleme, auf die im Bericht verwiesen werde, nicht kleinreden, weise jedoch darauf hin, dass es sich um spezifische Probleme gehandelt habe. Ein Beispiel seien digitale Wasserzähler, wobei es sich letztlich primär nicht um ein Datenschutzproblem gehandelt habe, sondern vielmehr um ein Problem, das das Thema „Unverletzlichkeit der Wohnung“ tangiere. Er schließe aus dem vorliegenden Bericht, dass das Thema bei den Landesbehörden und den Kommunen bereits einen hohen Stellenwert habe. Keiner der festgestellten Verstöße habe zu dem Ergebnis geführt, dass es Anlass gebe, sich politisch ernsthaft Sorgen machen zu müssen.

Anschließend äußerte er, wie auch aus dem Tätigkeitsbericht und den mündlichen Ausführungen des LfDI in den letzten Wochen hervorgehe, sei auf die Dienststelle des LfDI wesentlich mehr Arbeit zugekommen. Ihn interessiere, welche Ressourcen ihm zur Verfügung stünden, um präventiv tätig zu werden und in diesem

Zusammenhang beispielsweise die Menschen in Bezug auf den Umgang mit den eigenen Daten zu sensibilisieren. Denn er stelle immer wieder fest, dass es immer dann, wenn der Staat Daten erhebe, Aufregung gebe, während an anderer Stelle personenbezogene Daten relativ freizügig zur Verfügung gestellt würden. Aus seiner Sicht sei es wichtig, mit einer guten präventiven Arbeit und auch Öffentlichkeitsarbeit auf Problematiken aufmerksam zu machen; denn dadurch werde sicher auch missbräuchlicher Nutzung entgegengewirkt.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit teilte mit, der Tätigkeitsbericht sei vom Umfang her in der Tat nicht gewachsen. Während andere Landesdatenschutzbeauftragte ihre Tätigkeitsberichte häufig zum Anlass nähmen, vor dem Hintergrund von Einzelfällen die ganze Bandbreite zu schildern, was zu Tätigkeitsberichten im Umfang von mehreren Hundert Seiten führe, habe er das Ziel gehabt, sich auf grundlegende und übergreifende Fragestellungen zu fokussieren. Er habe nicht vor, künftig wesentlich umfangreichere Tätigkeitsberichte vorzulegen, es sei denn, vonseiten des Landtags würde es gewünscht.

Ihm seien systematische Aspekte wichtig, und er könne das, was der Abgeordnete der SPD wahrgenommen habe, bestätigen. Im öffentlichen Bereich seien von seiner Dienststelle im Berichtszeitraum keine systematischen Verstöße gegen den Datenschutz festgestellt worden. Es gebe immer wieder Einzelfälle, in denen bestimmte Rechtsnormen anders ausgelegt würden, als seine Dienststelle es für richtig halte, oder in denen ein Einzelversagen festgestellt werden müsse, beispielsweise Neugieranfragen im Bereich der Polizei. Solche Einzelfälle ließen sich nie ganz vermeiden; es könne jedoch keine Rede davon sein, dass im öffentlichen Bereich jemand systematisch gegen Datenschutzanliegen verstoßen würde.

Es sei positiv anzumerken, dass es in sehr vielen öffentlichen Stellen ein hohes Datenschutzbewusstsein gebe.

Bereits bevor es die Datenschutz-Grundverordnung gefordert habe, hätten sehr viele Behörden behördliche Datenschutzbeauftragte bestellt, und deshalb sei dieses Thema vor Ort bereits gut verankert. Insofern teile er die Einschätzung des Abgeordneten der SPD.

Im nicht öffentlichen Bereich, also beispielsweise bei Unternehmen, sei die Situation grundsätzlich anders. Dort sei es tatsächlich so, dass es bestimmte Geschäftsmodelle gebe, die von Anfang an ganz hart an der Grenze des datenschutzrechtlichen Zulässigen angesiedelt seien und sich immer in einem datenschutzrechtlichen Konfliktbereich bewegten. In diesem Bereich sei eine Aufsicht notwendig. Denn bei diesen Unternehmen sei nicht von vornherein die Einsicht zu unterstellen, die Rechte anderer z. B. der Nutzer, der Mitarbeiter oder der Geschäftspartner zu respektieren. Durch die Möglichkeit, Bußgelder zu verhängen, stehe der zuständigen Aufsichtsbehörde nunmehr ein Mittel zur Verfügung, noch prägnantere Verfahren zu führen.

Die Prävention sei in der Tat das Wichtigste. Dort sollte der Schwerpunkt liegen. Dies könne seine Dienststelle aus Gründen der Arbeitsbelastung jedoch nicht sicherstellen. Auch nach der Datenschutz-Grundverordnung habe seine Dienststelle als Aufsichtsbehörde sogar verschärft die Aufgabe, den Beschwerden von Bürgerinnen und Bürgern nachzugehen, und zwar deswegen verschärft, weil sie dieses Verfahren innerhalb sehr kurzer Frist abschließen müsse und keine Verfahren „auf die lange Bank schieben“ dürfe. Ferner sei es zukünftig nicht mehr möglich, Bürgerinnen und Bürger auf den Rechtsweg zu verweisen und beispielsweise zu erklären, der Fall sei geprüft worden und für recht kompliziert befunden worden, sodass der betroffenen Person empfohlen werde, vor dem Arbeitsgericht gegen den Arbeitgeber zu klagen. Nunmehr müsse die Aufsichtsbehörde selbst ermitteln und abschließen.

Seine Dienststelle werde den Spagat schaffen, sowohl die Beratung als auch die Prävention zu bewältigen. Zu Letzterem zählten beispielsweise auch Veranstaltungen mit Bürgerinnen und Bürgern sowie Vortrags- und Schulungsveranstaltungen mit Verantwortlichen.

Abschließend betonte er, auch in anderen Ländern sei der Personalbestand der Landesdatenschutzbehörde im vergangenen Jahr erhöht worden, doch kein anderer Landesdatenschutzbeauftragter sei im vergangenen Jahr so gestärkt worden wie seine Dienststelle. Dies habe dazu geführt, dass seine Dienststelle, was das Verhältnis von Aufsichtspersonal zur Zahl der zu beaufsichtigenden Unternehmen angehe, nicht mehr ganz hinten, sondern im Mittelfeld zu finden sei.

Ein Abgeordneter der Grünen legte dar, in Bezug auf das vernetzte Fahren gebe es immer wieder neue Entwicklungen. Im vorliegenden Tätigkeitsbericht habe er dazu jedoch keine Aussage gefunden. Ihn interessiere, ob es aus Sicht der Automobilindustrie keinen Anlass gebe, auf die Datenschutzaufsichtsbehörde zuzugehen, und ob der Datenschutzaufsichtsbehörde die Datenschutzmaßnahmen, die derzeit avisiert würden, ausreichten.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit antwortete, das Thema „vernetztes Fahren“ sei in seiner Dienststelle sogar ein Schwerpunktthema, komme im Tätigkeitsbericht wegen seiner Wichtigkeit jedoch nicht im Bereich Verkehr vor, sondern bei den Schwerpunktthemen, konkret unter Punkt 1.6. Seine Dienststelle fühle sich bei diesem Thema aus ihrer Sicht sehr gut durch die Unternehmen eingebunden, die das in besonderer Weise betreffe. Im vergangenen Jahr sei es im Übrigen gelungen, mit den großen Unternehmen eine sehr schöne Beratungsebene zu etablieren. Dazu gehörten die sogenannten Quartalsgespräche mit Daimler, in denen unabhängig von irgendwelchen Beschwerden oder anderen Anliegen darüber gesprochen werde, welche Planungen es gebe und welche Schritte in Sachen Automatisierung oder Datenverarbeitung geplant seien. Auf diese Weise erhalte seine Dienststelle Gelegenheit, zu Entwicklungen frühzeitig eine Meinung zu äußern und darzulegen, ob sie sie für unproblematisch oder möglicherweise schwierig halte.

Dies sei im vergangenen Jahr sehr gut angenommen worden und werde deshalb auch weitergeführt. Dies sei auch sinnvoll; denn das automatisierte Fahrzeug stoße in der Bevölkerung auf großes Interesse. Denn das Fahrzeug erhalte in Zukunft eine Vielzahl von Informationen über den Fahrer und über Fahrsituationen, und da seien auch sensible Informationen dabei. Ein Teilbereich seien beispielsweise die sogenannten Dashcams, also Anlagen zur Videoüberwachung aus dem Fahrzeug heraus. Er erinnere in diesem Zusammenhang daran, dass die modernen Fahrzeuge von vornherein drei, fünf oder häufig sogar noch mehr Videokameras hätten, beispielsweise für den Einparkassistenten oder bereits für die Gesamtbeobachtung des Verkehrsgeschehens.

Eine Innenraumüberwachung in Fahrzeugen spiele ebenfalls eine immer größere Rolle. Beispielsweise würden Gespräche mitgeschnitten, oder es gebe die Möglichkeit, das Fahrzeug oder bestimmte Funktionen per Sprachbefehl zu steuern. In diesem Zusammenhang hätten nicht nur die Unternehmen Interesse, mit seiner Dienststelle in Kontakt zu treten, sondern auch Bürgerinnen und Bürger, denen bewusst werde, dass es ein Unterschied sei, ob analog oder digital gefahren werde.

Ein Abgeordneter der Grünen äußerte, bekanntermaßen genossen die Parlamente wie auch der Landtag von Baden-Württemberg in Bezug auf die Anforderungen der Datenschutz-Grundverordnung eine privilegierte Position. Gleichwohl sei der Landtag nicht vollständig davon ausgenommen. Im Landtag gebe es eine Datenschutzordnung, die sicherlich etwas in die Jahre gekommen sei. Ihn interessiere, was der Landesbeauftragte für den Datenschutz und die Informationsfreiheit dem Landtag hinsichtlich einer Anpassung der Datenschutzordnung des Landtags empfehlen würde.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit erklärte, hierzu verweise er auf das, was er bereits in vielen bilateralen Gesprächen mit den Fraktionen des Landtags erklärt habe. Die Datenschutz-Grundverordnung entfalte in Bezug auf die parlamentarischen Abläufe im Landtag keinerlei Wirkung auf den Landtag und die Fraktionen. Allerdings gebe es auch innerhalb der Fraktionen bestimmte Verwaltungstätigkeiten. Dort gelte auch zukünftig das Landesdatenschutzgesetz. Die Datenschutzordnung, die sich der Landtag für den parlamentarischen Bereich selbst gegeben habe, fuße im Wesentlichen auf den damaligen Standardvorgaben sowohl des BDSG als auch des LDSG. Er könne dem Landtag nur

schwer Empfehlungen aussprechen, würde es jedoch für nicht fernliegend halten, angesichts dessen, dass sich die datenschutzrechtlichen Vorgaben für alle öffentlichen Stellen, für alle Unternehmen und auch für Privatpersonen wesentlich geändert hätten, darüber nachzudenken, für den eigenen Bereich bei der Datenschutzordnung entsprechend nachzulegen. Wenn der Landtag zu dem Schluss komme, so vorzugehen, sei er sehr gern bereit, zu beraten und zu unterstützen.

Der Ausschussvorsitzende erklärte, damit sei die Beratung zum Teil Datenschutz abgeschlossen.

Im Folgenden gehe es um den Teil Informationsfreiheit.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit führte aus, der vorliegende Tätigkeitsbericht sei der erste Tätigkeitsbericht für den Bereich Informationsfreiheit. Dies hänge damit zusammen, dass Baden-Württemberg mit dem Informationsfreiheitsgesetz im Vergleich zu den anderen Ländern etwas später gestartet sei. Die Grundbotschaft im Bereich der Informationsfreiheit laute, dass die Idee der Informationsfreiheit praktisch nicht mehr aufzuhalten sei, dass aus seiner Sicht jedoch in vielen Bereichen ein skeptischer Blick feststellbar sei und immer intensiver die Frage gestellt werde, wo die Grenzen der Informationsfreiheit lägen.

Eine ganz zentrale und wichtige Botschaft im Bereich Informationsfreiheit sei wieder einmal vom Bundesverfassungsgericht gekommen, das im Juni 2017 erstmals und sehr deutlich gesagt habe, dass es sich beim Zugangsrecht zu Informationen in der öffentlichen Verwaltung, also der Informationsfreiheit, um ein Grundrecht handle. Es habe also sowohl das Datenschutzgrundrecht als auch das Informationsfreiheitsgrundrecht noch einmal gestärkt und betont.

Eine zweite aus seiner Sicht sehr positive Entwicklung sei, dass immer mehr deutsche Länder inzwischen Informationsfreiheitsgesetze oder sogar Transparenzgesetze hätten. Kürzlich habe das Land Hessen ein eigenes Informationsfreiheitsgesetz auf den Weg gebracht und damit die „rote Laterne“ von Baden-Württemberg übernommen. Denn das hessische Informationsfreiheitsgesetz sei in Bezug auf den Regelungsbereich, die Ausnahmetatbestände und die Bedingungen, unter denen Bürgerinnen und Bürger von ihren Rechten Gebrauch machen könnten, mit Sicherheit das zurückhaltendste Informationsfreiheitsgesetz, das es in Deutschland gegeben habe. Diese „rote Laterne“ habe bisher Baden-Württemberg mit seinem Informationsfreiheitsgesetz gehabt.

Doch auch wenn die Skepsis tatsächlich steige, sei die Idee der Informationsfreiheit nicht aufzuhalten, und zwar auch deshalb nicht, weil es auch aufgrund der technischen Entwicklung immer naheliegender und plausibler werde, dass die öffentliche Verwaltung die Informationen, die sie habe, auch teile. Durch die Zugänglichkeit und die Macht des Internets sei es überhaupt kein Problem mehr, flächendeckend und sehr wirksam über öffentliche Themen aus Sicht einer Verwaltung zu berichten. Es sei überhaupt kein Problem mehr, die Mitwirkung der Bürgerinnen und Bürger anzustoßen, und es sei im Übrigen auch kein Problem mehr, tatsächlich eine neue Form der Verwaltungskontrolle zu etablieren. Denn Bürgerinnen und Bürger, die sich im Einzelfall informieren könnten, könnten auf diesem Wege durchaus auch Fälle von Korruption oder von Machtmissbrauch aufdecken, so sie denn vorlägen.

Die Nutzung der Möglichkeiten des digitalen Zeitalters durch die öffentliche Verwaltung sei also absolut naheliegend. Ein Land wie Baden-Württemberg, das eine eigene Digitalisierungsstrategie habe, könne sich im Bereich der Transparenz der öffentlichen Verwaltung nicht zurückhalten.

Dennoch steige ganz offensichtlich die Skepsis gegenüber dem Instrument Informationsfreiheit, was daran zu erkennen sei, dass es immer wieder Versuche gebe, bestimmte Bereiche der öffentlichen Verwaltung von dieser generellen Transparenzpflicht auszunehmen. Er nenne beispielsweise die Bereiche Verfassungsschutz, Rechnungshof, die Schulen und schulischen Einrichtungen sowie die Universitäten, die in bestimmten Bereichen ausgenommen seien. Dies seien Bereichsausnahmen, die in den frühen Informationsfreiheitsgesetzen, die es seit 1998 gebe,

überhaupt nicht zu finden seien. Die Idee, dass Beschränkungen eingebaut werden müssten, sei erst im Laufe der Zeit aufgekommen und sei im hessischen Informationsfreiheitsgesetz in gewisser Weise kulminiert.

Die Skepsis steige auch, was die Kosten der Informationsfreiheit angehe, weil gerade im kommunalen Bereich sichtbar werde, mit welchen Belastungen im Einzelfall Informationsfreiheit verbunden sein könne. Hierzu sei festzustellen, dass die ersten Anstrengungen der öffentlichen Verwaltung, bürgernah und bürgerfreundlich zu sein und sich zu öffnen, gerade im kommunalen Bereich gemacht worden seien und dass die Mittelbehörden oder auch das eine oder andere Ministerium tatsächlich mehr zu lernen gehabt hätten als die einzelne Kommune.

Insgesamt drohe aus seiner Sicht der Schwung, den die Informationsfreiheit in den letzten Jahren mit sich gebracht habe, zu erlahmen und drohe die Bereitschaft, die öffentliche Verwaltung grundsätzlich transparent zu machen, deutlich nachzulassen. Als Gegenmittel stehe eine verstärkte Beratung von Bürgerinnen und Bürgern zur Verfügung. Seine Dienststelle habe eine ganze Reihe von Bürgerveranstaltungen zum Thema Informationsfreiheit durchgeführt. Der Schwerpunkt habe im Berichtszeitraum jedoch auf der Beratung von Behörden gelegen. Seine Dienststelle habe im Bereich Informationsfreiheit alle Ministerien und alle Regierungspräsidenten beraten und führe stetig mit Kommunen sehr viele Informationsveranstaltungen durch. Auch dabei zeige sich eine deutliche Perspektive. Die Vorbehalte gerade in den Reihen der öffentlich Bediensteten gegenüber der Informationsfreiheit seien umso stärker, je weniger sie sich mit dem Instrument befasst hätten. Wenn seine Dienststelle in der Lage sei, vor Ort Aufklärungsarbeit zu leisten, spreche sich aus seiner Sicht bei den meisten herum und bleibe das Gefühl übrig, dass es sehr wohl möglich sei, das Thema Informationsfreiheit in den Griff zu bekommen, ohne dass es zu stark belaste.

Verbesserungen in Bezug auf die Informationsfreiheit könnten insbesondere durch Veränderungen in Bezug auf die Gebühren erzielt werden. Das Thema Gebühren sei im baden-württembergischen Informationsfreiheitsgesetz so streng geregelt wie in kaum einem anderen Informationsfreiheitsgesetz. Es gebe weder eine Obergrenze, noch gebe es den Ansatz, die Bearbeitung von Anfragen grundsätzlich gebührenfrei zu stellen. Aus seiner Sicht sei dies in gewisser Weise widersprüchlich. Wenn die Vorteile der Informationsfreiheit gesehen würden, nämlich Mitwirkung der Bürgerinnen und Bürger sowie bessere Kontrolle der Verwaltung, dann sei es nicht ganz nachvollziehbar, warum die Bürgerinnen und Bürger, die diesen Weg gingen und Informationsfreiheitsanträge gestellt hätten, auch noch mit Gebühren belastet werden sollten.

Seine zunächst nur ausschnittsweise Umfrage habe ergeben, dass sich der Umfang der Gebühren, die über die Informationsfreiheit tatsächlich eingenommen würden, landesweit im fünfstelligen Bereich bewege. Dies sei nicht so viel, als dass darauf nicht verzichtet werden könnte.

In Bezug auf die Gebührenfreiheit von Anträgen müsse in erster Linie der psychologische Aspekt in den Fokus genommen werden, dass, wenn einem Antragsteller relativ frühzeitig signalisiert werde, was seine Anfrage wohl kosten werde, mancher Antragsteller in der Erwartung, vielleicht 200 oder 300 € zahlen zu müssen, die Anfrage zurückziehe, was zu einer Entlastung aufseiten der Behörde führe. Wie auch in der Rechtsprechung deutlich werde, würden Gebühren in bestimmten Bereichen ganz offensichtlich dazu eingesetzt, um abzuschrecken. Wenn es im Einzelfall auch einmal um 5 000, 10 000 oder 15 000 € gehe, habe dies durchaus eine abschreckende Wirkung. Er sehe Bedarf für eine Diskussion darüber, warum Behörden glaubten, dieses Abschreckungsinstrument behalten zu müssen, und ob andere Wege gefunden werden könnten, damit Behörden mit der Informationsfreiheit ihren Frieden schlossen.

Wie er auch im schriftlichen Tätigkeitsbericht ausgeführt habe, habe er einen Ratgeber für Behörden und auf der anderen Seite für Bürgerinnen und Bürger herausgegeben, in welchem dargelegt werde, wie mit der Informationsfreiheit sinnvoll umgegangen werde, und zwar in dem Sinne, dass beide Seiten gut zueinander fänden. Wenn dem Bürger klar sei, dass er seine Anfrage möglichst konkret stellen solle und sich darauf beschränken sollte, was er wirklich wissen wolle, und wenn den Behörden aufgezeigt werde, wie dem Informationsanspruch mit relativ gerin-

gem Aufwand entsprochen werden könne, sei allen gedient. Auch dafür fänden sich im Tätigkeitsbericht Nachweise.

Abschließend erklärte er, es stehe eine Evaluierung des Informationsfreiheitsgesetzes an. Er bitte dringend darum, dass dies möglichst gut vorbereitet auf den Weg gebracht werde. Er habe bereits zum gegenwärtigen Zeitpunkt eine Menge Vorschläge, wie dieses Gesetz verbessert werden könne.

Ein Abgeordneter der SPD äußerte, bei Anfragen auf der Grundlage des Informationsfreiheitsgesetzes spiele, wie er auch selbst schon erfahren habe, häufig auch die Frage des Urheberrechts eine Rolle, wenn es um Gutachten gehe. Es gebe wohl eine Selbstverpflichtung der Landesregierung oder einzelner Ministerien, dass sie, wenn Gutachten in Auftrag gegeben würden, in den entsprechenden Verträgen mit denjenigen, die die Gutachten erstellen sollten, festschrieben, dass das Urheberrecht ausgeschlossen werde. Somit könne die Regierung mit gutem Beispiel vorangehen und einen wesentlichen Hinderungsgrund, der im Gesetz stehe, umgehen, sodass dem Bürger eine umfassende Einsichtnahme ermöglicht werden könne. Ihn interessiere, ob der Landesbeauftragte für den Datenschutz und die Informationsfreiheit im Rahmen seiner Beratungstätigkeit einen Überblick darüber erhalten habe, wie weit die Ministerien und Regierungspräsidien in Bezug auf die Gestaltung ihrer Verträge in dieser Hinsicht bereits vorangeschritten seien und wie die Ministerien zu dieser Vorgehensweise stünden.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit legte dar, das Urheberrecht könne in der Tat ein wichtiges Gegenrecht zu Informationszugangsanträgen sein. Der Ansatz, bereits beim Einkauf eines Gutachtens klarzumachen, dass mit der Vorlage des Gutachtens auch die Rechte in Bezug auf die Informationsfreiheit zu übertragen seien, sodass entsprechend beauskunftet werden dürfe und möglicherweise sogar veröffentlicht werden dürfe, sei ein sehr wichtiger und guter Ansatz. Einen Überblick darüber, inwieweit im Land insgesamt bereits so verfahren werde, habe er jedoch nicht.

In der praktischen Arbeit gebe es eine relativ einfache Form, mit dem Urheberrecht zurechtzukommen, und diese beruhe darauf, dass das Urheberrecht nicht ausschließe, dass Akteneinsicht genommen werde. Das Urheberrecht diene dem Schutz des geistigen Eigentums und nehme insbesondere die unberechtigte Veröffentlichung in den Fokus, schließe jedoch nicht aus, dass die Behörde den Antragsteller zu sich bitte und ihm die Möglichkeit einräume, das Gutachten zu lesen. Der Antragsteller dürfe das Gutachten allerdings nicht mitnehmen und auch nicht selbst ins Internet stellen.

Im Einzelfall komme es darauf an, mit wie viel Fingerspitzengefühl damit umgegangen werde. Es wäre eine Verletzung des Urheberrechts, wenn der Bürger mit dem Gutachten allein gelassen würde und die Möglichkeit hätte, es komplett abzufotografieren und dann ins Internet zu stellen, aber es sei zulässig, dass er sich Notizen mache oder sich Auszüge vollständig zur Kenntnis bringe. Darüber müsse aufgeklärt werden, und seine Dienststellen mache Kommunen, die keinen Überblick über solche Spezialfragen hätten, klar, in welchem Korridor sie sich bewegen dürften.

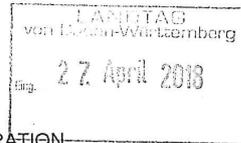
Dies sei eine praktikable Vorgehensweise, doch die angesprochene generelle Lösung, die eine Weiterverbreitung von Gutachten ermögliche, sei besser.

Der Ausschussvorsitzende bedankte sich für die Berichte.

Der Ausschuss beschloss als Empfehlung an das Plenum ohne förmliche Abstimmung, von der Mitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit von Baden-Württemberg vom 18. Januar 2018, Drucksache 16/3290, und der vom Innenministerium hierzu mit Schreiben vom 26. April 2018 vorgelegten Stellungnahme der Landesregierung (*Anlage 1*) sowie von der Mitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit vom 21. Februar 2018, Drucksache 16/3600, Kenntnis zu nehmen.

13. 06. 2018

Reinhold Gall

**Anlage 1****Baden-Württemberg**
 MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION  
 DER MINISTER


Innenministerium Baden-Württemberg • Pf. 10 34 65 • 70029 Stuttgart

 An die  
 Präsidentin des Landtags  
 von Baden-Württemberg  
 Frau Muhterem Aras MdL  
 Haus des Landtags  
 Konrad-Adenauer-Straße 3  
 70173 Stuttgart

I

 Datum **26. April 2018**  
 Durchwahl 0711 231-3227  
 Aktenzeichen 2-0557.6/11  
 (Bitte bei Antwort angeben)

*U. Ver*  
*U. Ver*  
*U. Ver*
**33. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz**  
 Stellungnahme der Landesregierung

 Anlagen  
 Stellungnahme der Landesregierung  
 Synopse

Sehr geehrte Frau Landtagspräsidentin,

*liebe Frau Aras,*

die Landesregierung hat in der Kabinettsitzung am 10. April 2018 die Stellungnahme zum 33. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz (LT Drs. 16/3290) beschlossen.

Ich darf Ihnen diese Stellungnahme und eine Synopse in der Anlage zuleiten.

Je 35 Mehrfertigungen der Stellungnahme und der Synopse werden der Landtagsverwaltung für die Beratung im Ständigen Ausschuss mit gesonderter Post übersandt.

Mit freundlichen Grüßen

Thomas Strobl

\*) Die oben genannte Synopse kann beim Informationsdienst des Landtags eingesehen werden.



# Baden-Württemberg

MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION

## **Stellungnahme der Landesregierung**

**zum**

### **33. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg (LT-Drs. 16/3290)**

- 2 -

Die Landesregierung nimmt im Folgenden – entsprechend dem Beschluss des Landtags vom 17. September 1987 (LT-Drs. 9/4667) – zu den Beanstandungen sowie zu den sonstigen wesentlichen Ausführungen des Landesbeauftragten für den Datenschutz Stellung, die den Datenschutz im öffentlichen Bereich betreffen.

Da die Landesregierung keine Möglichkeit hat, auf die Einhaltung datenschutzrechtlicher Vorschriften durch nicht-öffentliche Stellen hinzuwirken, äußert sie sich zu den Ausführungen des Landesbeauftragten für den Datenschutz in diesem Bereich nur, soweit es um Fragen der Gesetzgebung oder das Verhalten der Landesregierung geht und eine Erwidern erforderlich ist. Dasselbe gilt für sonstige Bereiche des Datenschutzes, soweit das Land Baden-Württemberg nicht zuständig ist.

## **1. Schwerpunkte**

### 1.2 Sicher oder frei – zwischen Skylla und Charybdis?

Der Landesbeauftragte für den Datenschutz wiederholt in seinem Tätigkeitsbericht einzelne Kritikpunkte zu den im vergangenen Jahr beschlossenen Änderungen des Polizeigesetzes. Neue Gesichtspunkte werden in diesem Zusammenhang nicht vorgebracht. Das Innenministerium hält die in der Polizeigesetz-Novelle aus dem Jahr 2017 geschaffenen Rechtsgrundlagen für in der Sache notwendig, in ihrer Reichweite angemessen und verfassungsrechtlich zulässig. Bereits Wilhelm von Humboldt wusste: „Denn ohne Sicherheit ist keine Freiheit“. Angesichts der anhaltend hohen abstrakten Gefährdung in Deutschland und auch in Baden-Württemberg sieht das Innenministerium seine Pflicht darin, der Polizei – neben einer guten Ausstattung – die notwendigen rechtlichen Instrumente dafür zu geben, die Bürgerinnen und Bürger möglichst gut beschützen zu können.

Dies gilt ganz besonders für die Terrorismusbekämpfung, aber eben auch für Maßnahmen gegen schwere – z.B. organisierte – Kriminalität. Da Terroristen auf eine hohe Mobilität und eine moderne Kommunikation angewiesen sind, stellen v.a. die Quellen-Telekommunikationsüberwachung und die elektronische Aufenthaltsüberwachung (sog. elektronische „Fußfessel“) zentrale Instrumente zur polizeilichen Abwehr schwerer Gefahren dar. Dabei orientieren sich die neuen Regelungen eng an den vom Bundesverfassungsgericht in seiner BKA-Entscheidung aufgestellten Grenzen, indem weitreichende Anforderungen an Transparenz, individuellen Rechtsschutz und datenschutzrechtliche Kontrolle beachtet und notwendige Löschungspflichten vorgesehen sind.

- 3 -

Im Einzelnen:

#### Zur Telekommunikationsüberwachung - § 23b Polizeigesetz (PolG)

Der Wortlaut der Vorschrift orientiert sich eng an den vom Bundesverfassungsgericht aufgestellten Anforderungen an die zu treffende Prognoseentscheidung bezüglich einer Gefahrenlage im Vorfeld einer konkreten Gefahr. Eine Einschränkung von § 23b Absatz 1 Satz 1 Nummer 1 PolG auf die Abwehr von Gefahren des internationalen Terrorismus wird nicht für erforderlich erachtet. Mit der weiteren Voraussetzung einer dringenden und erheblichen Gefahr wird nämlich sichergestellt, dass eine Gefährdung der genannten Rechtsgüter hinreichend absehbar ist. Bei einer solch konkreten und dringenden Gefahrenlage für besonders gewichtige Rechtsgüter ist eine entsprechende Telekommunikationsüberwachung auch für nicht-terroristische Gefahren als verhältnismäßig anzusehen. Entscheidend ist schließlich das zu schützende Rechtsgut und nicht das Motiv für dessen Gefährdung.

#### Zur elektronischen Aufenthaltsüberwachung - § 27c PolG

Es ist richtig, dass die mittels elektronischer Aufenthaltsüberwachung erhobenen Daten nach § 27c Absatz 2 Satz 3 Nummer 4 PolG auch zur Abwehr einer erheblichen gegenwärtigen Gefahr für das Leben, die körperliche Unversehrtheit oder die persönliche Freiheit Dritter verwendet werden können. Andernfalls würde ein erheblicher Vertrauensverlust in die Funktionsfähigkeit der Polizei und damit der staatlichen Institutionen insgesamt drohen, wenn trotz einer elektronischen Aufenthaltsüberwachung die entsprechenden Daten nicht zur Verhinderung erheblicher Straftaten, insbesondere von schweren Gewaltstraftaten, genutzt werden dürften. Daher teilt das Innenministerium die Kritik des Landesbeauftragten für den Datenschutz nicht.

### 1.3 „Und Action!“ – Zunahme der Videoüberwachung in allen Lebensbereichen

#### 1.3.6 Videoüberwachung durch öffentliche Stellen

Beim Polizeipräsidium Mannheim wird seit April 2007 der Bereich des Hauptbahnhofvorplatzes mit drei Kameras videoüberwacht. Die überwachte Fläche erstreckt sich auf ca. einen Hektar, dies entspricht etwa 0,6% des innerstädtischen Bereichs. Die Kriminalitätsbelastung pro Hektar im Überwachungsbereich, gemessen an den Delikten der Straßen-

- 4 -

und Rauschgiftkriminalität, ist im Vergleich zur sonstigen innerstädtischen Belastung ca. dreißigfach höher.

Trotz teilweise erheblicher Störanfälligkeit des Systems gelang es im Jahr 2017, wiederholt Straftaten durch Videobeobachtung festzustellen und Interventionskräfte schnell heranzuführen. Hierbei handelte es sich vorrangig um Körperverletzungsdelikte und Sachbeschädigungen.

### 1.7 Digitalisierung im Gesundheitswesen

Die ausführliche Darstellung des Themas Digitalisierung im Gesundheitswesen ist zutreffend. Gerade auch für den Gesundheits- und Pflegebereich, der von digitalen Entwicklungen in immer größeren Schritten erfasst wird, bietet die fortschreitende Digitalisierung Herausforderungen, aber auch erhebliche Chancen, um eine qualitätsorientierte medizinische, psychotherapeutische und pflegerische Versorgung der Menschen in Baden-Württemberg auch in Zukunft zu gewährleisten und noch weiter zu verbessern. Es handelt sich dabei um ein zusätzliches Angebot zur bestehenden Versorgung. Ein direkter Kontakt zwischen Patientinnen/Patienten und Ärztinnen/Ärzten ist weiterhin nicht nur möglich, sondern in vielen Fällen auch notwendig. Der Tätigkeitsbericht des Landesbeauftragten für den Datenschutz weist explizit auf den Förderauftrag Digitalisierung in Medizin und Pflege und die gute Abstimmung hin. Nicht nur in der Ausschreibung zum Förderauftrag wurde explizit auf die Einhaltung der den Datenschutz betreffenden Rechtsvorschriften hingewiesen, auch in den Zuwendungsbescheiden durch das Ministerium für Soziales und Integration findet sich dies wieder.

Aus Sicht des Ministeriums für Soziales und Integration ist es zu begrüßen, dass Projekte in diesem Bereich das Angebot des Landesbeauftragten für den Datenschutz annehmen, um gemeinsam datenschutzkonforme Lösungen zu entwickeln, wie vereinzelt bereits auch geschehen.

### 1.8 Digitalisierung in Schulen – Smarte Bildung

#### 1.8.3 „Schicks doch via Messenger“ – Wie private Endgeräte und „Soziale Medien“ die Schulwelt verändern ...

Wie der Landesbeauftragte für den Datenschutz zutreffend feststellt, sehen sich Schulen vermehrt dem Druck ausgesetzt, die verlockenden und einfach zu bedienenden Funktiona-

- 5 -

litäten, die Soziale Netzwerke und Messenger bieten, einzusetzen. Das Kultusministerium ist sich über die datenschutzrechtliche Problematik bewusst, die mit der Nutzung dieser Technik einhergeht. In einer Handreichung zum Einsatz von "Sozialen Netzwerken" an Schulen (sog. „Facebook-Verbot“) hat das Kultusministerium bereits im Jahre 2013 auf diese Technik reagiert und klargestellt, dass insbesondere die Verwendung von Sozialen Netzwerken für die dienstliche Verarbeitung personenbezogener Daten generell verboten ist. Hierunter fällt jegliche dienstlichen Zwecken dienende Kommunikation zwischen Schülern und Lehrkräften sowie zwischen Lehrkräften untereinander, ferner das (Zwischen-)Speichern von personenbezogenen Daten jeder Art auf Sozialen Netzwerken. In verschiedenen weiteren Handreichungen hat das Kultusministerium erläutert, was aus datenschutzrechtlicher Sicht zu berücksichtigen ist, wenn Apps wie Soziale Netzwerke, Messenger usw. eingesetzt werden sollen. Der datenschutzkonforme Umgang ist zudem Bestandteil von Fortbildungsmaßnahmen für Lehrkräfte.

## **2. Innere Sicherheit**

### 2.2 Besondere Zeiten

#### 2.2.1 Kompetenzzentrum zur Koordinierung des Präventionsnetzwerks gegen (islamistischen) Extremismus in Baden-Württemberg (KPEBW)

Der Landesbeauftragte für den Datenschutz weist hinsichtlich der Zusammenarbeit zwischen dem externen Beratungsdienstleister Violence Prevention Network (VPN) und den baden-württembergischen Sicherheitsbehörden zu Recht darauf hin, dass deren Datenaustausch im Rahmen von Fallkonferenzen zu Personen des islamistischen Spektrums unter bestimmten rechtlichen Voraussetzungen zulässig ist, eine ausreichende Regelungslage jedoch fehlt. Da es sich bei VPN um einen bundesweit aktiven Anbieter handelt, wäre nach Ansicht des Innenministeriums die Anpassung des Bundesdatenschutzgesetzes (BDSG) erforderlich. Diese Notwendigkeit wurde zwischenzeitlich erkannt. Daher wird derzeit eine Ergänzung des BDSG auf Bundesebene geprüft. Dieses Vorhaben wird seitens des Innenministeriums begrüßt und unterstützt, wenngleich das Innenministerium die Auffassung vertritt, dass trotz der verbesserungswürdigen Rechtslage die Zusammenarbeit mit VPN – inklusive der datenschutzbezogenen Aspekte – in Baden-Württemberg unter Einhaltung der rechtlichen Voraussetzungen erfolgt und deren Fortsetzung daher unproblematisch möglich ist.

### 2.2.2 Projekt SonAR BW

Das Innenministerium ist der Auffassung, dass das Vorgehen von der geltenden Regelung des § 38 Absatz 1 PolG gedeckt ist. Soweit vom Landesbeauftragten für den Datenschutz kritisiert wird, dass im Projektverlauf die Datendurchsicht nicht unmittelbar der Verbrechensbekämpfung diene, sondern erst die Voraussetzungen dafür geschaffen wurden, ist einzuwenden, dass auch darin eine vorbeugende Verbrechensbekämpfung zu sehen ist. Hat die Polizei personenbezogene Daten im Rahmen eines Strafermittlungsverfahrens gewonnen, kann sie nach § 38 Absatz 1 PolG diese Daten grundsätzlich nutzen, soweit dies zur Gefahrenabwehr oder zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Die Nutzung zur vorbeugenden Bekämpfung von Straftaten ist bis zu einer Dauer von zwei Jahren erforderlich, wenn aufgrund tatsächlicher Anhaltspunkte der Verdacht besteht, dass die betroffene Person eine Straftat begangen hat (§ 38 Absatz 2 Satz 1 PolG). Innerhalb dieser zwei Jahre sind gerade keine tatsächlichen Anhaltspunkte dafür erforderlich, dass die Person zukünftig Straftaten begehen wird.

Bei der Recherche in POLAS BW handelte es sich nach Auffassung des Innenministeriums damit nicht um eine „Datennutzung ins Blaue hinein“, sondern um eine zulässige Nutzung rechtmäßig gespeicherter Daten.

### 2.2.3 Erhebung personenbezogener Daten unbegleiteter minderjähriger Ausländer (UMA) bei Jugendämtern

Die erkennungsdienstliche Behandlung unbegleiteter minderjähriger Ausländer (UMA) durch die Polizei und die damit im Zusammenhang stehenden Vorbereitungsmaßnahmen des Landeskriminalamtes (LKA) waren nach Ansicht des Innenministeriums rechtmäßig. Insbesondere war die Polizei berechtigt, vor einer durchzuführenden erkennungsdienstlichen Behandlung zu prüfen, welche Personen hierzu vorgeladen werden müssten. Durch die Polizei erkennungsdienstlich behandelt werden dürfen grundsätzlich alle illegal ins Bundesgebiet eingereisten UMA. Die Klärung der Frage, welche UMA bereits erkennungsdienstlich behandelt worden sind und welche nicht, diene damit allein der Vermeidung nicht notwendiger Grundrechtseingriffe bei den Betroffenen.

Die Zuständigkeit des LKA für den im Vorfeld durchgeführten Datenabgleich ergibt sich aus § 11 Nummer 8 der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes (DVO PolG). Danach ist das LKA dafür zuständig, Personenfeststellungsverfahren durchzuführen, soweit seine Einrichtungen hierzu erforderlich sind oder die Mitwirkung

- 7 -

des Bundeskriminalamtes (BKA), eines anderen Landeskriminalamtes oder einer ausländischen Polizeidienststelle erforderlich ist. Vorliegend war im Wege der Auftragsdatenverarbeitung – weil schneller und mangels persönlicher Kenntnisnahme durch konkrete Beamte weniger eingriffsintensiv – ein automatisierter Abgleich durch das BKA erforderlich; dies fällt nach der genannten Vorschrift in den Zuständigkeitsbereich des LKA.

Das Innenministerium ist im Rahmen seiner Aufgabenerfüllung an einem offenen und vertrauensvollen Umgang mit dem Landesbeauftragten für den Datenschutz interessiert und hatte diesen daher eigeninitiativ vor Durchführung des Projekts SonAR BW informiert. Eine gleichermaßen offene Kommunikation erfolgte auf Nachfrage des Landesbeauftragten für den Datenschutz zur Registrierung unbegleiteter minderjähriger Ausländer (UMA).

#### 2.2.4 Die Reichsbürger und der Verfassungsschutz

Die im Zusammenhang mit der Meldepraxis der Kommunen von Erkenntnissen zu „Reichsbürgern und Selbstverwaltern“ an das Landesamt für Verfassungsschutz (LfV) geäußerte Kritik, dass nach der bisherigen Übermittlungsvorschrift in § 9 Absatz 1 des Landesverfassungsschutzgesetzes (LVSG) die Gemeinden von der Übermittlungsbefugnis an das LfV ausgenommen waren, ist wiederholt vom Landesbeauftragten für den Datenschutz geltend gemacht worden. Aus Sicht des Innenministeriums ist diese Auffassung nicht überzeugend, da nichts auf eine bewusste Ausnahme der Kommunen durch den Gesetzgeber hindeutet. Im Interesse der Normenklarheit und der Bestimmtheit stellt nunmehr § 9 Absatz 1 LVSG mit der Änderung, die am 8. Dezember 2017 in Kraft getreten ist, klar, dass die Landesbehörden im weiteren Sinne – und damit auch die Kommunen – zur Übermittlung verpflichtet werden. Die Formulierung orientiert sich an § 1 Absatz 1 des Landesverwaltungsverfahrensgesetzes.

#### 2.3 Was es sonst noch gab

##### 2.3.1 Zuverlässigkeitsüberprüfung

Das Innenministerium erarbeitet derzeit eine umfassende Novellierung des Polizeigesetzes, um die Richtlinie (EU) 2016/680 umzusetzen. In diesem Zusammenhang wird auch geprüft, ob eine entsprechende gesetzliche Regelung zur Durchführung von Zuverlässigkeitsüberprüfungen in das Polizeigesetz aufgenommen werden kann. Parallel hierzu hat das Innenministerium Gespräche mit dem Landesbeauftragten für den Datenschutz über

die nähere Ausgestaltung von landeseinheitlichen Einwilligungserklärungen aufgenommen.

### 2.3.2 Bodycam

Zutreffend ist, dass die Möglichkeit des Pre-Recordings erst im Laufe des Gesetzgebungsverfahrens in die Rechtsgrundlage zur Nutzung der Bodycam aufgenommen wurde und dass in der verabschiedeten Fassung für die Stufe des Pre-Recordings lediglich auf das Vorliegen einer allgemeinen Gefahr abgestellt wird. Für die dauerhafte Speicherung blieb es dagegen stets beim Erfordernis einer Gefahr für Leib oder Leben von Personen. Ohne diese Voraussetzung bleiben die im Pre-Recording gewonnenen Daten unverwertbar und werden gelöscht. Hintergrund für die abgestufte Gefahrenschwelle ist die erforderliche Abgrenzung des Pre-Recordings zur dauerhaften Speicherung. Das Pre-Recording soll gerade dazu dienen, erste Eskalationsstufen wie z.B. verbale Provokationen zu erfassen, die in der Folge erst zu einer Gefahr für Leib oder Leben einer Person führen können.

Im Rahmen der Anwendererprobung von Bodycams bei der Polizei im Jahr 2017 konnte festgestellt werden, dass in rd. 70 % der Einsatzfälle bereits die Aktivierung des Pre-Recordings ausreichend war, um eine präventive Wirkung zu erzielen. Neben weiteren Fällen, in denen bereits die Ankündigung des Pre-Recordings ausreichte, um eine Beruhigung der Situation zu erreichen, trug gerade die Nutzung des Pre-Recordings entscheidend dazu bei, in der Mehrzahl der Fälle auf eine über 60 Sekunden hinausgehende Datenspeicherung (dauerhafte Aufzeichnung) verzichten zu können. Insofern wird die Bewertung der „Überflüssigkeit des Pre-Recordings“ im Hinblick auf den Gesamtprozess zur Reduzierung von Gewalt gegen Polizeibeamte durch das Innenministerium nicht geteilt. Würden die Anforderungen an das Pre-Recording erhöht, käme es zu Abgrenzungsschwierigkeiten mit der Gefahrenschwelle der dauerhaften Speicherung, womit der Zweck des Pre-Recordings ins Leere liefe.

### 2.3.4 Kontrolle der Falldatei Rauschgift

Bei der Kontrolle der Falldatei Rauschgift durch den Landesbeauftragten für den Datenschutz wurden einzelne Speicherungen festgestellt, bei denen die rechtlichen Voraussetzungen für eine Speicherung nicht vorlagen; diese Speicherungen wurden umgehend gelöscht. Nach Einschätzung des Innenministeriums handelt es sich dabei um Einzelfälle; strukturelle Mängel sind hierbei nicht feststellbar.

- 9 -

Der Umfang des zur Prüfung vorgelegten Aktenrückhalts war – wie vom Landesbeauftragten für den Datenschutz dargestellt – in der Tat sehr unterschiedlich. Dies lag jedoch weniger an der dezentralen Speicherzuständigkeit als vielmehr an Kommunikationsdefiziten im Vorfeld der Kontrolle.

Bezüglich der Frage der Dokumentation von Prognoseentscheidungen ist unstrittig, dass Prognoseentscheidungen einzelfallbezogen begründet werden müssen, wobei diese Begründung nachvollziehbar dokumentiert sein muss. Während der Landesbeauftragte für den Datenschutz der Auffassung ist, diese Dokumentation sei in POLAS BW vorzunehmen, ist das Innenministerium der Ansicht, dass die Dokumentation auch im Papieraktenrückhalt erfolgen darf. Gestützt wird diese Auffassung auf eine Entscheidung des Verwaltungsgerichtshofs Baden-Württemberg (VGH), in der festgestellt wird, dass die im entschiedenen Fall notwendige Prognose einer Wiederholungsgefahr in den vorgelegten (Papier-)Akten nicht feststellbar sei (Urteil vom 10.02.2015, Az. 1 S 554/13, Randnummer 85, zitiert nach juris). Daraus lässt sich aber schließen, dass die Dokumentation auch dort erfolgen darf, sonst wäre diese Feststellung im Urteil entbehrlich.

Ebenfalls unterschiedliche Auffassungen bestehen bezüglich der Frage, ob Dokumentationsmängel geheilt werden können oder nicht. Der Landesbeauftragte für den Datenschutz geht davon aus, dass Rechtsfolge von Dokumentationsmängeln zwingend eine Löschung der Daten sein müsse. Das Innenministerium vertritt die Auffassung, dass eine erneute Speicherung desselben Falles möglich sein muss, wenn die Voraussetzungen des § 8 Absatz 2 Bundeskriminalamtgesetz (BKAG) für eine Speicherung der entsprechenden Daten nach der Löschung weiterhin vorliegen und insbesondere eine Negativprognose (ohne Berücksichtigung neu erworbenen Wissens und ggf. unter Berücksichtigung der Tatsache, dass der Betroffene seither nicht mehr polizeilich in Erscheinung getreten ist) weiterhin getroffen werden kann. Bejaht man die Möglichkeit einer hypothetischen Neuspeicherung, so spricht aber viel dafür, eine Heilungsmöglichkeit für Dokumentationsmängel zu bejahen. Denn das Datenschutzrecht dient nicht dazu, ein Fehlverhalten des speichernden Sachbearbeiters zu sanktionieren, sondern den Bürger vor nicht gerechtfertigten Eingriffen in sein Grundrecht auf informationelle Selbstbestimmung zu schützen.

Demgegenüber steht das Interesse der Allgemeinheit an einer effektiven Gefahrenabwehr durch die Polizei – im konkreten Fall bei der Falldatei Rauschgift Täter betreffend, die bereits Straftaten mit einem erheblichem Unrechtsgehalt begangen haben und bei denen eine Wiederholungsgefahr tatsächlich besteht. Für diese Rechtsauffassung spricht darüber hinaus Folgendes: Der VGH zitiert in seiner o.g. Entscheidung u.a. ein Urteil des

- 10 -

Oberverwaltungsgerichts des Saarlandes. Die dort maßgebliche Vorschrift zur Löschung personenbezogener Daten bei unrechtmäßiger Speicherung unterscheidet sich jedoch an einer Stelle entscheidend von den Vorschriften im baden-württembergischen Polizeigesetz und im Landesdatenschutzgesetz (LDSG). Nach § 38 Absatz 2 Satz 1 Nummer 1 des Saarländischen Polizeigesetzes (SPolG) sind personenbezogene Informationen immer dann zu löschen, wenn bereits „ihre Speicherung unzulässig war“. § 46 Absatz 1 Satz 1 Nummer 1 PolG setzt aber – wie auch § 23 Absatz 1 Nummer 1 LDSG – voraus, dass „die Speicherung unzulässig ist“. Daraus kann man schließen, dass ein Lösungsanspruch bei unzulässiger Speicherung zwar entsteht, aber mit Heilung des Mangels wieder erlischt.

Unabhängig davon wurden und werden Maßnahmen ergriffen, um den Sachbearbeiterinnen und Sachbearbeitern die Notwendigkeit einzelfallbezogener Begründungen zu verdeutlichen.

#### 2.3.5 SKB-Datenbank

Die Darstellung im Tätigkeitsbericht ist zutreffend. Nach eingehender Prüfung, ob der Szene-Fotograf zu Recht in dieser Datei gespeichert war, mussten die Daten des Betroffenen wegen der mangelhaften Dokumentation der Gründe, die für die Speicherung maßgeblich waren, gelöscht werden. Eine Speicherung der personenbezogenen Daten in diesem Einzelfall wäre rechtlich zulässig gewesen, sofern eine ausreichende Dokumentation erfolgt wäre. Um eine hohe Datenqualität zu gewährleisten und die Anwender der Arbeitsdatei Szenenkundige Beamte für die Problemstellungen bei der Speicherung in der Datenbank erneut zu sensibilisieren, wurden Schulungsmaßnahmen durch das Innenministerium durchgeführt.

#### 2.3.6 Vergabe fünfjähriger Laufzeit bei einem Fall geringer Bedeutung

Bei dem im Tätigkeitsbericht angeführten Einzelfall ging es um die Speicherberechtigung personenbezogener Daten aus der erkennungsdienstlichen Behandlung eines Beschuldigten aus dem Jahr 2008. Diesem lag ein Verfahren wegen des Verdachts der gefährlichen Körperverletzung zu Grunde, das vom zuständigen Amtsgericht nach § 153a Strafprozessordnung (StPO) eingestellt worden war. Im Rahmen der Auskunftserteilung an den Landesbeauftragten für den Datenschutz wurden die gespeicherten Daten vollständig mitgeteilt. Als letzte Tat war hierbei eine Körperverletzung aus dem Jahr 2013 erfasst, bezüglich derer das Ermittlungsverfahren nach § 170 Absatz 2 StPO eingestellt worden war. Aufgrund der vorhandenen elf Vortaten (wiederholte Sachbeschädigungen, Körperverlet-

- 11 -

zungsdelikte, Urkundenfälschung und Verstoß gegen das Betäubungsmittelgesetz) und eines bestehenden Tatverdachtes für das Körperverletzungsdelikt im Jahr 2013 wurde seitens des betroffenen Polizeipräsidiums eine Negativprognose für den Betroffenen gestellt und die Tat aus dem Jahr 2013 mit einer Speicherfrist von fünf Jahren geführt. Der Landesbeauftragte für den Datenschutz sah in den Taten jedoch insgesamt nur Straftaten von geringer Bedeutung und kritisierte die gewählte Speicherfrist. Der Rechtsauffassung, dass nicht nur die wiederholten Tatbegehungen, sondern auch die Art und Schwere der Tatvorwürfe sowie der Umstand, dass es sich bei drei Tatvorwürfen um Körperverletzungsdelikte handle, eine verkürzte Speicherfrist nicht angezeigt erscheinen ließen, schloss sich der Landesbeauftragte für den Datenschutz nicht an.

Nach telefonischer Erörterung der Sach- und Rechtslage mit dem Landesbeauftragten für den Datenschutz schloss sich das betroffene Polizeipräsidium abschließend seiner Bewertung des Einzelfalles an. Die beanstandeten Daten wurden gelöscht.

#### 2.3.7 Datenlöschung aufgrund unzureichend begründeter Negativprognose

Die Daten des Vorgangs wurden, wie im Tätigkeitsbericht dargestellt, vollständig gelöscht. Aktenbestand ist nicht mehr vorhanden. Nur aus der Erinnerung von Beamten des betroffenen Polizeipräsidiums kann daher mitgeteilt werden, dass die Daten des hier vorliegenden Einzelfalles unberechtigt gespeichert und daher zu löschen waren. Begründet wurde dies mit der mangelnden Dokumentation der Wiederholungsgefahr und damit mit einer Entscheidung des VGH Baden-Württemberg (Urteil vom 10.02.2015, Az. 1 S 554/13), wonach eine solche Dokumentation zwingend erforderlich ist und die entsprechende Prognoseentscheidung in den Akten nachvollziehbar zu dokumentieren ist.

Der Vorgang wurde seinerzeit durch die zuständige Datenstation des Polizeipräsidiums mit dem Ergebnis geprüft, dass die Daten durch den Sachbearbeiter ohne Begründung und folglich auch ohne Dokumentation der Wiederholungsgefahr gespeichert wurden. Da die Datenspeicherung damit tatsächlich unberechtigterweise erfolgte, wurde der Datensatz gelöscht.

Um solche Einzelfälle zu vermeiden, ist das oben genannte Urteil des VGH Baden-Württemberg bezüglich der Begründung und Dokumentation der Wiederholungsgefahr Gegenstand von Fortbildungsmaßnahmen.

## 4. Verkehr

### 4.1 MoveBW

Das frühzeitige Einbinden des Landesbeauftragten für Datenschutz durch das Projekt moveBW hat sich als wertvoll und richtig erwiesen. So konnten gleich zu Projektbeginn wichtige Hinweise berücksichtigt werden. Gerade in frühen Entwicklungsphasen muss der Grundstein für Informationsschutz und Datensicherheit eines Systems gelegt werden, da spätere Anpassungen oft sehr aufwändig oder nicht mehr möglich sind (Privacy by design). Das Projekt moveBW wurde von Anfang an auf Datensparsamkeit ausgelegt. Im Sinne des Informationsschutzes werden nur die Daten erhoben, die zur Erfüllung der angebotenen Dienste notwendig sind. Der Nutzer selbst wählt die gewünschte Servicetiefe. Die dafür benötigten personenbezogenen Daten werden dem Nutzer jederzeit transparent gemacht.

Am Ende des Entwicklungsprozesses steht die Prüfung der Systemsicherheit durch eine neutrale, externe Instanz. Durch die sogenannten „Penetration Tests“ wird das Risiko auf unberechtigten Datenzugriff von außen minimiert.

Im Projekt moveBW hat Informationsschutz und Datensicherheit einen hohen Stellenwert und wird von den Projektpartnern aktiv gelebt.

### 4.3 Echt-Bodensee-Card

Der Landesbeauftragte für den Datenschutz äußert Bedenken zum datenschutzrechtlichen Konzept der Deutschen Bodensee Tourismus GmbH bei der Gästekarte und hat eine grundlegende Überarbeitung der Datenschutzbestimmungen empfohlen.

Das Innenministerium ist von dieser unter dem Abschnitt „Verkehr“ aufgeführten Thematik nicht unmittelbar berührt, weist jedoch ergänzend auf Folgendes hin:

Durch Gesetz vom 7. November 2017 wurde die Kurtaxeregelung im Kommunalabgabengesetz (KAG) geändert. Nach § 43 Absatz 3 Nummer 3 KAG kann nun durch Satzung geregelt werden, dass die zur Erhebung der Kurtaxe erforderlichen Daten elektronisch an die Gemeinde zu übermitteln sind; dabei sind Bestimmungen über die Daten und das Übermittlungsverfahren zu treffen. Bei der elektronischen Übermittlung ist ein sicheres Verfah-

- 13 -

ren zu verwenden, das den Datenübermittler authentifiziert und die Vertraulichkeit und Integrität des Datensatzes gewährleistet.

Der Landesbeauftragte für den Datenschutz wurde im Rahmen der Anhörung beteiligt und hatte zur Gesetzesänderung keine Anmerkungen.

#### 4.4 Überlassung von Rohmessdaten aus Geschwindigkeitsmessungen an private Sachverständige

Seit Vorliegen des Schreibens des Landesbeauftragten für den Datenschutz vom 16. Februar 2017 (Eingang bei der Zentralen Bußgeldstelle am 20. März 2017) verlangt das zuständige Regierungspräsidium Karlsruhe von Sachverständigen keine Datenschutzerklärungen mehr. Die Sachverständigen erhalten die Messreihe nunmehr allerdings nur noch aufgrund richterlichen Beschlusses.

Wird ein Sachverständiger von einem Verteidiger beauftragt und verlangt dieser die gesamte Messreihe, so wird dies verweigert. Daraufhin stellt der Verteidiger in der Regel einen Antrag auf gerichtliche Entscheidung, der sodann dem zuständigen Amtsgericht vorgelegt wird. Die Richter entscheiden generell dahingehend, dass die Messreihe zur Verfügung zu stellen ist. Liegt der Beschluss vor, übersendet das Regierungspräsidium Karlsruhe die Messreihe ohne Datenschutzerklärung.

Diese Vorgehensweise bedeutet sowohl für das Regierungspräsidium Karlsruhe als auch für die Gerichte Mehrarbeit, entspricht jedoch den Vorgaben des Landesbeauftragten für den Datenschutz.

#### 4.5 Geschwindigkeitsmessungen bei Gemeinden durch Private

Zuständig für die Verfolgung von Ordnungswidrigkeiten sind die Bußgeldbehörden als untere Verwaltungsbehörden (§§ 26 Absatz 1 StVG, 36 Absatz 1 OWiG, §§ 2 Absatz 1, 5 Absatz 1 Nummer 7 OWiGZuVO). Neben den Landratsämtern und den Großen Kreisstädten als örtliche Straßenverkehrsbehörden besteht eine parallele Zuständigkeit der Gemeinden als Ortschaftspolizeibehörden gemäß §§ 61 Absatz 1 Nummer 4, 62 Absatz 4, 66 Absatz 2 PolG. Die zuständige Bußgeldbehörde ist jedoch „Herrin des Verfahrens“.

Die jeweiligen Behörden können sich bei ihrer Aufgabenerfüllung nur für einfache (technische) Hilfsarbeiten beauftragter Dritter bedienen. In Übereinstimmung mit Abschnitt 2 des

- 14 -

33. Tätigkeitsberichts zu Nummer 4.5 sind die wesentlichen Schritte des Bußgeldverfahrens von den zuständigen Behörden selbst wahrzunehmen. In jedem Fall muss der hoheitliche Kernbereich gewahrt werden, da Verstöße gegen die Straßenverkehrs-Ordnung (StVO) bußgeldbewehrt sind und es hierdurch in der Regel zu Eingriffen in die Rechte Dritter kommt. Daher ist die Verfolgung und Ahndung von Ordnungswidrigkeiten im Straßenverkehr den Behörden und Polizeidienststellen als Hoheitsträger vorbehalten. Die von den privaten Unternehmen dokumentierten Verstöße unterliegen der rechtlichen Prüfung durch die zuständigen Behörden, ob diese zureichende tatsächliche Anhaltspunkte für den Tatbestand einer Ordnungswidrigkeit bieten. Unter Anwendung des Opportunitätsprinzips entscheidet die zuständige Behörde im Rahmen ihres pflichtgemäßen Ermessens, ob und gegen wen sie ein Bußgeldverfahren einleitet (Entschließungs- und Auswahlermessen). Private Unternehmen dürfen mithin nicht selbstständig über die Einleitung eines Bußgeldverfahrens entscheiden.

## **5. Justiz**

### **5.1 Einführung der elektronischen Gerichtsakte**

Im Vorfeld der Pilotierung der elektronischen Akte in der Justiz Baden-Württembergs wurde im Jahr 2016 ein ergänzendes Datensicherheits- und Datenschutzkonzept erstellt, das auf weitere Dokumente referenziert. Es ergänzt dabei das umfassende Datensicherheits- und Datenschutzkonzept, das der bisherige Outsourcing-Partner erstellt hatte, im Hinblick auf die neuen Anforderungen der elektronischen Aktenführung.

Selbstverständlich sind diese Dokumente in einem einheitlichen Konzept zusammenzuführen, zu konsolidieren und weiterzuentwickeln, das den Wechsel vom Outsourcing zur IT Baden-Württemberg (BITBW) ebenso umfasst wie die neuen Aspekte der elektronischen Aktenführung. Dies ist jedoch zu integrieren in die ressortübergreifende Neuausrichtung der Landesverwaltung zum Thema Informationssicherheit. In diesem Rahmen wird die Informationssicherheit gesamtheitlich und konsequent nach den neuen Standards des Bundesamtes für Sicherheit in der Informationstechnik sowie den neuen Richtlinien des Informationssicherheitsbeauftragten für die Landesverwaltung Baden-Württemberg etabliert werden.

## 5.2 Längerfristige verdeckte Videoüberwachung im Rahmen eines Ermittlungsverfahrens

Die Sachverhaltsdarstellung ist zutreffend. Das Ministerium der Justiz und für Europa ist in Übereinstimmung mit dem Landesbeauftragten für den Datenschutz der Auffassung, dass für die in Rede stehende konkrete Ermittlungsmaßnahme nach § 163f Absatz 3 StPO eine richterliche Anordnung bzw. Bestätigung erforderlich gewesen wäre, auch wenn die rechtliche Bewertung der zuständigen Staatsanwaltschaft, die Ermittlungsmaßnahme auf § 100h Absatz 1 Nummer 1, Absatz 2 Satz 2 Nummer 1 StPO zu stützen, nicht unvertretbar erschien. Wie das Ministerium der Justiz und für Europa dem Landesbeauftragten für den Datenschutz bereits mit Schreiben vom 19. Juni 2017 mitgeteilt hatte, hat der Leitende Oberstaatsanwalt der zuständigen Staatsanwaltschaft Vorsorge dafür getroffen, dass bei vergleichbaren Konstellationen künftig eine richterliche Anordnung erwirkt werden wird.

## 6. Kommunales

### 6.3 Sog. Jedermann-Einwendungen bei der Öffentlichkeitsbeteiligung im Rahmen der Bauleitplanung

Die Darstellung des Landesbeauftragten für den Datenschutz ist zutreffend. Die rechtliche Beurteilung wird geteilt.

Die im Rahmen der Öffentlichkeitsbeteiligung eingegangenen schriftlichen Stellungnahmen Privater müssen den beschlussfassenden Gremien grundsätzlich unverfälscht, d.h. ohne Kürzungen oder Korrekturen zur Verfügung gestellt werden. Die Gemeinde ist allerdings verpflichtet, die in den Stellungnahmen enthaltenen personenbezogenen Daten auf das datenschutzrechtlich Erforderliche zu beschränken. Dies gilt auch für die Präsentation und die Vorlagen in öffentlicher Sitzung. Die in dem Tätigkeitsbericht dargestellte Lösung der Verwendung von Kennziffern stellt dafür eine gute Möglichkeit dar.

### 6.4 Das widerspenstige Landratsamt

Die Darstellung des Landesbeauftragten für den Datenschutz ist zutreffend. Die rechtliche Beurteilung wird geteilt.

Ein Ortsvorsteher ist als ständiger Stellvertreter des Bürgermeisters bei der Leitung der örtlichen Verwaltung für die sachgemäße Erledigung der Aufgaben, den ordnungsgemäßen Ablauf und die innere Organisation der Ortsverwaltung zuständig. Ein Vertretungs-

- 16 -

oder Sachentscheidungsrecht, das über den Vollzug der Beschlüsse des Ortschaftsrats hinausgeht, besitzt er nur, wenn ihn der Bürgermeister nach § 53 Absatz 1 Gemeindeordnung (GemO) mit solchen Befugnissen ausgestattet hat.

Nach den vorliegenden Informationen umfasst die örtliche Verwaltung in der Stadt nicht die Zuständigkeit für die Ortspolizeibehörde. Ein oben erwähntes Vertretungs- oder Sachentscheidungsrecht wurde den Ortsvorstehern durch den Bürgermeister nicht eingeräumt. Auch die Hauptsatzung der Stadt enthält keine abweichende Regelung, sondern gibt lediglich den Gesetzeswortlaut des § 71 GemO wieder.

Eine gesetzliche Regelung, wonach der Ortsvorsteher kraft Gesetzes „organschaftlicher Vertreter der Ortspolizeibehörde“ ist, besteht in der Form nicht.

Dass bei Fehlen einer eigenständigen Funktionseinheit Ortspolizeibehörde in den Teilortsverwaltungen – wie vom Landratsamt ausgeführt – der Ortsvorsteher der einzige örtliche Vertreter der Ortspolizeibehörde sei und sich ggf. des Ordnungsamts im Hauptort als zentraler Stelle bedienen könne, ist vom Gesetzeswortlaut nicht gedeckt: Nach § 71 Absatz 3 GemO vertritt der Ortsvorsteher kraft Gesetzes den Bürgermeister nur bei dem Vollzug der Beschlüsse des Ortschaftsrats (hier nicht einschlägig) und bei der Leitung der örtlichen Verwaltung. Deren Umfang wird aber nach § 68 Absatz 4 GemO festgelegt – örtliche Verwaltung ist somit nicht kraft Gesetzes der Teil der Gemeindeverwaltung, der die Ortschaft betrifft, sondern es ist vielmehr von der Entscheidung des Bürgermeisters abhängig, welche Aufgaben von der örtlichen Verwaltung erledigt werden. Sie ist bloße Organisationseinheit der Gemeindeverwaltung. Sich im Übrigen der Gemeindeverwaltung zu bedienen, ist dem Ortsvorsteher speziell für den Vollzug der Beschlüsse des Ortschaftsrats gestattet, für darüber hinausgehende Angelegenheiten besteht auf gesetzlicher Grundlage jedenfalls kein Raum.

Das zuständige Landratsamt hat mitgeteilt, dass die Rechtsauffassung künftig beachtet wird und die zuständigen Mitarbeiter hierüber informiert werden. Weitergehende Maßnahmen sind nicht erforderlich.

- 17 -

## **7. Gesundheit und Soziales**

### 7.3 Arztpraxen im Internet

### 7.4 Messenger bei Ärzten und Pflegekräften

Nach Auskunft der Landesärztekammer Baden-Württemberg werden im Zusammenhang mit der Verordnung (EU) 2016/679 die "Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der ärztlichen Praxis", die die Bundesärztekammer gemeinsam mit der Kassenärztlichen Bundesvereinigung herausgibt, derzeit überarbeitet. Das Kapitel "Sicherheitsvorkehrungen bei externer elektronischer Kommunikation" ist die aktuellste Quelle, die zu dieser Thematik herangezogen werden kann und als Information für die Mitglieder der Landesärztekammer dient.

Auch wird im Rahmen der Fortbildungsveranstaltungen, die derzeit für die Mitglieder der Landesärztekammer im Zusammenhang mit dem Inkrafttreten der Verordnung (EU) 2016/679 angeboten werden, auf die genannten Themen eingegangen.

Die Landesärztekammer hat ihrerseits Rücksprache mit der Kassenärztlichen Vereinigung Baden-Württemberg gehalten. Ihr wurde mitgeteilt, dass dort keine speziellen Veröffentlichungen zu den genannten Themen existieren. Die Landesärztekammer nimmt die Hinweise des Landesbeauftragten für den Datenschutz zum Anlass, ihre Mitglieder für die angesprochene Thematik zu sensibilisieren.

### 7.5 Datenschutz in Pflegeeinrichtungen

Die im Tätigkeitsbericht angesprochenen sogenannten Biografiegespräche mit Bewohnern von stationären Pflegeeinrichtungen zielen darauf ab, bei deren Pflege und Versorgung die individuellen Interessen und Gewohnheiten zu berücksichtigen sowie auf besondere Bedürfnisse und Wünsche einzugehen. Richtig ist, dass es dabei nicht primär um die Lebensgeschichte geht, sondern um aktuelle Umstände und Befindlichkeiten, die im Rahmen der täglichen Betreuung von Relevanz sind. Hierbei spielen alle Themen eine Rolle, die eine Auswirkung auf das tägliche Leben der einzelnen Bewohnerin/des einzelnen Bewohners haben. Dies können vielfältige Fragen aus den Bereichen Essen, Körperpflege, Kleidung, Hobbys, Religion, kulturelle Individualität sowie der sexuellen und geschlechtlichen Identität sein. Auf diese Weise soll dem individuellen Wohlbefinden, der Lebensqualität, der Selbständigkeit, der Selbstbestimmtheit und der Selbstverantwortung von Menschen, die in stationären Pflegeeinrichtungen leben, in höchstmöglichem Maße Rechnung getra-

- 18 -

gen werden. Wichtig ist, dass das Gespräch nicht schematisch, sondern unter Rücksichtnahme auf die Persönlichkeit und erkennbare Bedürfnisse im Kontext mit der konkreten Situation durchgeführt wird und dem Betroffenen vermittelt wird, dass er auf Fragen, die besonders sensible Aspekte seiner Persönlichkeit betreffen, nicht antworten muss. Dies gilt in besonderem Maße, wenn das Gespräch anhand von Vordrucken geführt wird.

Auch das Ministerium für Soziales und Integration hält es für unerlässlich, darauf hinzuwirken, dass stationäre Pflegeeinrichtungen, die moderne Funktechnologie (RFID) nutzen, um in ihrer Orientierungsfähigkeit eingeschränkte Bewohnerinnen und Bewohner am Verlassen der Einrichtung zu hindern, sich eingehend mit den einschlägigen rechtlichen und insbesondere datenschutzrechtlichen Fragestellungen auseinandersetzen.

Das Ministerium für Soziales und Integration wird in seiner Funktion als oberste Heimaufsichtsbehörde die angesprochenen Sachverhalte zum Anlass nehmen, die unteren Heimaufsichtsbehörden im Rahmen von Dienstbesprechungen für die betreffenden Fragestellungen zu sensibilisieren und diese zu bitten, bei den in stationären Pflegeeinrichtungen durchzuführenden Prüfungen besonderes Augenmerk hierauf zu legen.

Die geplante Herausgabe eines Kataloges für häufig gestellte Fragen („FAQ“) zum Thema Datenschutz im Pflegebereich wird ausdrücklich begrüßt.

#### 7.6 Kontroll- und Beratungsbesuch bei einer Betriebskrankenkasse

Die geprüfte Betriebskrankenkasse hat dem Landesbeauftragten für den Datenschutz zugesagt, die Kamera abzubauen.

Das Ministerium für Soziales und Integration führt die Rechtsaufsicht über die landesunmittelbaren Krankenkassen in Baden-Württemberg. Da der Prüfungsvorgang nach Auskunft des Landesbeauftragten für Datenschutz noch nicht vollständig abgeschlossen ist, wurde die betroffene Betriebskrankenkasse bislang nicht namentlich benannt. Sollte es sich bei der geprüften Betriebskrankenkasse um keine landesunmittelbare Krankenkasse handeln, würde die Bewertung des Sachverhalts der jeweils zuständigen Aufsichtsbehörde obliegen. Auf Grund der Nichtnennung der Krankenkasse besteht seitens der Rechtsaufsicht derzeit kein Anlass, diese Angelegenheit aufsichtsrechtlich zu verfolgen.

## 7.8 Einwilligungserklärungen bei Sozialämtern

Der Einschätzung des Landesbeauftragten für Datenschutz ist zuzustimmen.

Das Ministerium für Soziales und Integration wird die anderen Sozialhilfeträger auf die Problematik hinweisen.

## 8. Schule und Hochschulen

### 8.1 Schlüssel ist out – Transponder ist in! Elektronische Schließanlagen an Schulen und was sie alles könn(t)en

Das Kultusministerium schließt sich der datenschutzrechtlichen Bewertung des Landesbeauftragten für den Datenschutz vollumfänglich an. Dieses Thema ist an Schulen nicht neu. Immer häufiger erneuern die Schulträger die bisher üblichen mechanischen Schließanlagen in Schulgebäuden und tauschen diese durch elektronische Schließsysteme aus. Kern der Schließanlage ist die Verwaltungssoftware. Sie enthält den Schließplan, der festlegt, welche Türen mit welchen Schlüsseln geöffnet werden können. In der Regel werden hier auch Informationen über die Schlüsselinhaber verwaltet.

Nach § 48 Absatz 2 Schulgesetz (SchulG) errichtet und unterhält der Schulträger im Rahmen seiner Zuständigkeit für die äußeren Schulangelegenheiten das Schulgebäude, dazu gehört auch der Einbau und der Betrieb einer elektronischen Schließanlage. Wird für eine Schule eine elektronische Schließanlage betrieben, ist der Schulträger für die personenbezogene Datenverarbeitung verantwortlich. Sofern der Schulträger die Verwaltung der Schließanlage auf den Schulleiter delegiert, ändert dies nichts an seiner datenschutzrechtlichen Verantwortung, da der Schulleiter gemäß der Anordnungen des Schulträgers handelt (§ 41 Absatz 1 SchulG) und an dessen Weisungen gebunden ist. Der Schulträger ist auch in der Pflicht, die notwendigen technischen und organisatorischen Maßnahmen gemäß § 9 LDSG zu treffen, um Datenschutzverstöße zu vermeiden. Ferner muss er sicherstellen, dass nur die erforderlichen Daten im Sinne der Datensparsamkeit und Datenvermeidung verarbeitet werden.

Das Kultusministerium hat den Kommunalen Landesverbänden als Vertreter der Schulträger eine Handreichung zum Versand an deren Mitglieder zur Verfügung gestellt. Diese Handreichung empfiehlt, möglichst nur Schließanlagen-Systeme zu verwenden, die lediglich die Wirkung eines Schlüssels haben und nur den Zutritt zu den Schulgebäuden ge-

- 20 -

währen, wobei insbesondere keine gewährten oder abgelehnten Zutrittsversuche protokolliert werden.

#### 8.4 Zur Vorlage der Zeugnishefte der Grundschule an die weiterführende Schule sowie Austausch der weiterführenden Schule und der Grundschule über Schüler

Im November 2017 wandte sich der Landesbeauftragte für den Datenschutz an das Kultusministerium und berichtete über Beschwerden, wonach weiterführende Schulen zu Beginn des aktuellen Schuljahres neben den vorzulegenden Dokumenten nach den entsprechenden Bestimmungen auch „Zeugnishefte der Grundschulen“ von den aufgenommenen Schülerinnen und Schülern verlangt hätten. Zugleich sei die Abgabe einer Einwilligungserklärung gefordert worden, um sich bei Beratungsgesprächen auch über einzelne Schülerinnen und Schüler austauschen zu können.

Nach Ansicht des Landesbeauftragten für den Datenschutz besteht keine Rechtsgrundlage dafür, dass aufnehmende Schulen sich generell die Zeugnishefte der Grundschulen vorlegen lassen; die freiwillige Vorlage sei allenfalls im Einzelfall auf Grundlage einer Einwilligung zulässig. Auch für ein generelles Einholen von Einwilligungen der Erziehungsberechtigten in ein Gespräch der aufbauenden Schulen mit der Grundschule über einen einzelnen Schüler bestehe keine Rechtsgrundlage.

Dem Kultusministerium ist ein harmonischer, möglichst bruchloser Übergang des einzelnen Schülers bzw. der einzelnen Schülerin von der Grundschule auf die weiterführende Schule besonders wichtig.

Im Interesse einer bestmöglichen Förderung der Schülerinnen und Schüler ist zum aktuellen Schuljahr bereits die Rechtsgrundlage für die verbindliche Vorlage der Grundschulempfehlung geschaffen worden.

Daneben lässt die aktuelle Rechtslage im vorliegenden Zusammenhang darüber hinaus zu, dass die Schulen auf der Grundlage von Einwilligungen die für die schulische Arbeit benötigten Daten erheben. Dies setzt voraus, dass im Einzelfall entsprechender Bedarf durch die Schulen etwa im Rahmen eines Beratungsgesprächs erkannt worden ist.

- 21 -

#### 8.5 Was darf die Duale Hochschule Ausbildungsstätten über Studierende mitteilen?

Das Wissenschaftsministerium hat die Anregungen des Landesbeauftragten für den Datenschutz zu § 12 Absatz 2 Satz 2 des Entwurfs eines Gesetzes zur Weiterentwicklung des Hochschulrechts (HRWeitEG) aufgegriffen und berücksichtigt. Sowohl der Gesetzentwurf als auch die Begründung wurden angepasst.

So ist im Einbringungsentwurf des HRWeitEG vom 9. Januar 2018 geregelt, dass nur Daten über den Zeitpunkt der Immatrikulation bzw. deren Widerruf, den Zeitpunkt der Exmatrikulation, den Zeitraum einer Beurlaubung, den Zeitpunkt der Feststellung des Verlusts des Prüfungsanspruchs und die Tatsache, dass Rechtsmittel gegen Entscheidungen der DHBW eingelegt wurden, an die Ausbildungsstätten übermittelt werden dürfen. Diese Informationen haben unmittelbare Auswirkungen auf das Vertragsverhältnis zwischen Studierenden und Ausbildungsstätten und u.U. auch auf das Rechtsverhältnis von Ausbildungsstätte und DHBW. Die vom Landesbeauftragten für den Datenschutz kritisierte, im Anhörungsentwurf vorgesehene Erlaubnis, Informationen über die Ladung zu Wiederholungsprüfungen weiterzugeben, wurde gestrichen. Die Erforderlichkeit und Verhältnismäßigkeit der Datenübermittlung wird in der Gesetzesbegründung ausführlich dargelegt.

#### 8.6 Langer Weg zur Auskunft

Der berichtete Umgang einer Hochschule mit einem Auskunftsverlangen eines ehemaligen Studierenden ist zutreffend dargestellt. Die Hochschule hat sich in ihrer Stellungnahme zur Beanstandung des Landesbeauftragten für den Datenschutz dessen Rechtauffassung angeschlossen und hat dem Studierenden Auskunft in schriftlicher Form erteilt. Außerdem hat sie zugesichert, dass sich vergleichbare Versäumnisse nicht wiederholen sollen. Das Wissenschaftsministerium hält die Rechtauffassung des Landesbeauftragten für den Datenschutz grundsätzlich für zutreffend. Es wird aber für möglich gehalten, dass künftige Fälle ab dem 25. Mai 2018 mit der Geltung der Verordnung (EU) 2016/679 wegen der dann geltenden neuen Rechtslage anders beurteilt werden könnten.